CA ARCserve® Central Host-Based VM Backup

Guia do Usuário

r16.5

Referências a produtos da CA Technologies

Este documento faz referência aos seguintes produtos da CA Technologies:

- CA ARCserve® Backup
- CA ARCServe® D2D
- CA ARCserve® Replication and High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

Entrar em contato com a CA

Para assistência técnica online e uma lista completa dos locais, principais horários de atendimento e números de telefone, entre em contato com o Suporte técnico pelo endereço http://www.ca.com/worldwide.

Links para suporte ao CA ARCserve Central Applications:

O CA Support online oferece um abrangente conjunto de recursos para solucionar seus problemas técnicos e fornece acesso fácil a importantes informações sobre o produto. Por meio do CA Support, você tem acesso fácil a consultas confiáveis que estão sempre disponíveis. Os links abaixo permitem acessar vários sites do CA Support disponíveis:

- **Entendendo o suporte --** O link abaixo fornece informações sobre programas de manutenção e ofertas de suporte, incluindo termos e condições, declarações, SLOs (Service-Level Objectives - Objetivos de Nível de Serviço) e horários de atendimento.

  https://support.ca.com/prodinfo/centappssupportofferings

- **Registrando-se para obter suporte --** O link abaixo o direciona para o formulário de registro online do CA Support que é usado para ativar o suporte ao produto.

  https://support.ca.com/prodinfo//supportregistration

- **Acessando o Suporte técnico --** O link abaixo o direciona à página de suporte ao CA ARCserve Central Applications.

  https://support.ca.com/prodinfo/arccentapps

Alterações na documentação

As seguintes atualizações na documentação foram feitas desde a última release do CA ARCserve Central Host-Based VM Backup:

- Atualizado para incluir comentários do usuário, aprimoramentos, correções e outras alterações secundárias para ajudar a melhorar a utilização o e a compreensão do produto ou da documentação.
- Criar diretivas de backup (na página 73) atualizado. Este tópico inclui agora duas novas opções na guia Configurações de backup/Avançado: Reservar espaço no destino e Catálogos e a guia Preferências/Alertas por email: dois novos alertas de Tarefa de mesclagem foram adicionados e Falha na mesclagem foi removida.
- O tópico Editar ou copiar diretivas de backup (na página 77) foi atualizado. Este tópico inclui agora duas novas opções na guia Configurações de backup/Avançado: Reservar espaço no destino e Catálogos.
- O tópico Exibir logs do CA ARCserve Central Host-Based VM Backup (na página 84) foi atualizado. Este tópico inclui agora duas novas opções na lista suspensa Módulo: Atualizar vários nós e Tarefa de mesclagem do CA ARCserve D2D.
- O tópico Recuperar uma máquina virtual inteira (na página 99) foi atualizado. Este tópico agora está atualizado para refletir o último design da caixa de diálogo.
- O tópico Erros de acesso negado ao atualizar os nós (na página 124) foi atualizado. Este tópico inclui agora duas soluções para desativar o UAC (User Account Control – Controle de Contas de Usuários).
- O tópico Executar recuperação bare metal (na página 155) foi atualizado. Este tópico foi atualizado agora para incluir o novo utilitário (Criar kit de inicialização para recuperação bare metal) para criar o ISO do WinPE para executar a BMR. Arquivos ISO não são mais fornecidos. Além disso, este tópico inclui também suporte para a BMR a partir de um backup realizado em uma máquina UEFI para uma máquina BIOS e de uma máquina BIOS para uma máquina UEFI.
- O tópico Como criar um kit de inicialização (na página 172) foi adicionado. Este tópico foi adicionado para incluir os novos recursos e funções do novo utilitário para criar imagens ISO do WinPE para executar a BMR.

  Observação: a opção Criar um kit de inicialização foi removida e substituída por este tópico.
- Atualizada a Restauração de aplicativo - Microsoft Exchange Server com os novos tópicos do cenário sobre Como restaurar um aplicativo do Microsoft Exchange. Este tópico agora inclui suporte do Exchange 2013, consulte Revisar os pré-requisitos e considerações de restauração.
- O tópico O CA ARCserve Central Host-Based VM Backup não reconhece os volumes nos discos dinâmicos ao recuperar a máquina virtual em um ESX Server ou Hyper-V Server alternativo (na página 152) foi adicionado. Esse tópico descreve a solução para recuperar os volumes em discos dinâmicos.

- O tópico Excluir arquivos da verificação do antivírus (na página 192) foi adicionado. Este tópico descreve os arquivos, as pastas e os processos a serem excluídos da verificação do antivírus.
- Os tópicos a seguir foram atualizados para fornecer credenciais internas ou do administrador de domínio para efetuar logon no sistema operacional convidado da máquina virtual.
  - Tarefas essenciais da instalação (na página 17)
  - Soluções para itens de verificação prévia (na página 59)
  - Erros de acesso negado ao atualizar os nós (na página 124)

Índice

Capítulo 1: Introdução ao CA ARCserve Central Host-Based VM Backup

Esta seção contém os seguintes tópicos:

Introdução

O CA ARCserve Central Applications combina as principais tecnologias de gerenciamento e proteção de dados com um ecossistema de aplicativos de destino que funcionam em uníssono para possibilitar proteção, cópia, movimentação e transformação de dados, no local e remotamente, em ambientes globais.

O CA ARCserve Central Applications é fácil de usar, gerenciar e instalar. Ele fornece às empresas controle automatizado de suas informações para tomarem decisões conscientes sobre o acesso, a disponibilidade e a segurança de seus dados, com base no valor comercial geral.

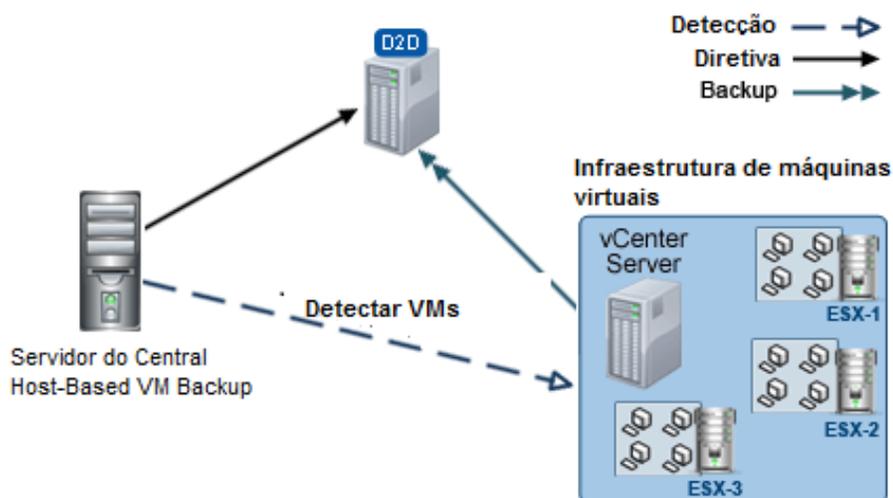
Sobre o CA ARCserve Central Host-Based VM Backup

Um dos CA ARCserve Central Applications é o aplicativo CA ARCserve Central Host-Based VM Backup. Este aplicativo funciona com o CA ARCserve D2D, que é uma solução de backup leve, e permite que você proteja várias máquinas virtuais sem a necessidade de instalar o software ou um agente em cada máquina virtual. Esse recurso minimiza os efeitos adversos da execução de várias operações de backup no mesmo servidor físico e permite executar backups em nível de arquivo, em nível de aplicativo ou BMR (Bare Metal Recovery - Recuperação Bare Metal) a partir dos backups das máquinas virtuais.

O CA ARCserve Central Host-Based VM Backup é facilmente dimensionado para que você possa adicionar máquinas virtuais, conforme a necessidade, sem precisar adquirir licenças adicionais ou instalar o software em todas as máquinas virtuais no ambiente de produção.

Como o CA ARCserve Central Host-Based VM Backup funciona

O CA ARCserve Central Host-Based VM Backup permite proteger máquinas virtuais em execução em um ESX ou vCenter Server em uma única passagem usando uma instância do CA ARCserve D2D instalada em um proxy. Use a lista de verificação a seguir para começar:

1. Instale o CA ARCserve D2D em uma máquina (física ou virtual) que atue como um proxy de backup no seu ambiente. Para obter instruções sobre a instalação, consulte o tópico Instalar o CA ARCserve D2D, extraído do Guia do Usuário do CA ARCserve D2D. Verifique se o proxy está configurado corretamente.
2. Adicionar nós a serem gerenciados. Especifique um servidor ESX e o aplicativo detecta as máquinas virtuais em execução que atendem aos requisitos.
3. Criar diretivas de backup. Em cada diretiva, especificar o proxy de backup, onde foi instalado o CA ARCserve D2D.
4. Atribua diretivas de backup a cada VM, para poder proteger todas as VMs com a única instância do CA ARCserve D2D em execução no proxy de backup.
5. Crie grupos de nós para gerenciar melhor o ambiente de máquinas virtuais. Por exemplo, é possível agrupar nós pela função de negócios ou pelo aplicativo instalado e atribuir uma diretiva configurada para proteger os nós associados a uma função específica ou os que são executados em um determinado aplicativo.

Biblioteca do CA ARCserve Central Applications

Os mesmos tópicos contidos no sistema de ajuda do CA ARCserve Central Applications também estão disponíveis como um Guia do Usuário em PDF. A versão mais recente deste guia e o sistema de ajuda podem ser acessados a partir da Biblioteca do CA ARCserve Central Applications.

Os arquivos de Notas da Versão do CA ARCserve Central Applications contém informações relacionadas aos requisitos do sistema, suporte ao sistema operacional, suporte à recuperação de aplicativos e outras informações que podem ser necessárias antes de instalar este produto. Além disso, estes arquivos contêm uma lista de problemas conhecidos os quais você deve saber antes de usar o CA ARCserve Central Applications. A versão mais recente de Notas da Versão pode ser acessada a partir da Biblioteca do CA ARCserve Central Applications.

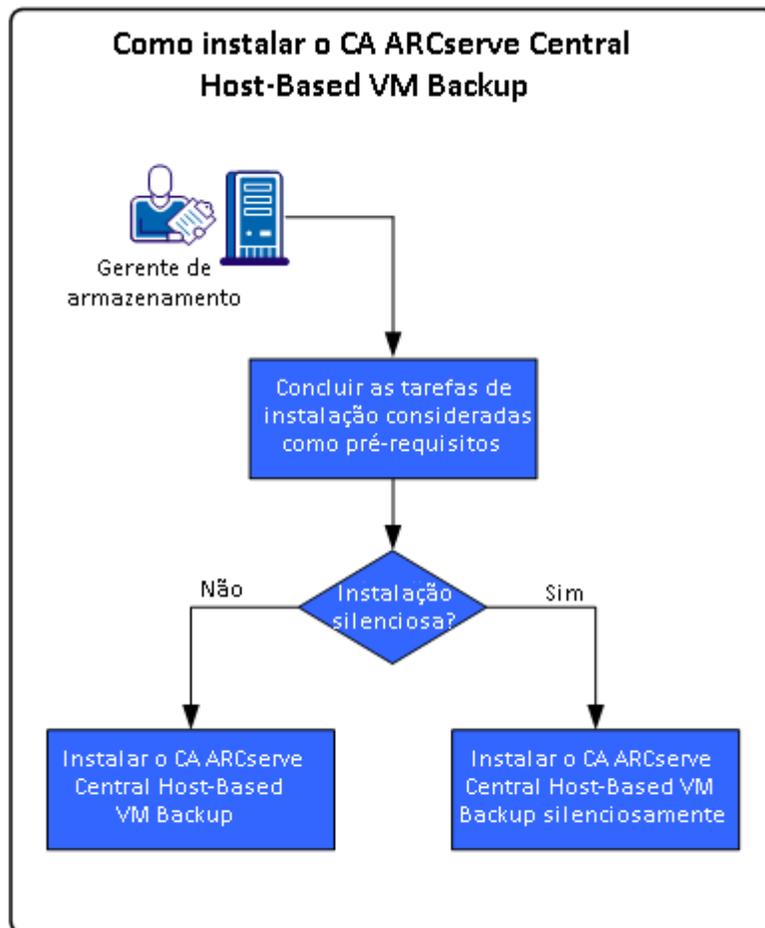
Capítulo 2: Instalação e configuração do CA ARCserve Central Host-Based VM Backup

Esta seção contém os seguintes tópicos:

Como instalar o CA ARCserve Central Host-Based VM Backup

Esse cenário descreve como os Gerenciadores de Armazenamento podem instalar o CA ARCserve Central Host-Based VM Backup usando os seguintes métodos:

- Instalação padrão -- este método usa o assistente de instalação para instalar o aplicativo.
- Instalação silenciosa -- este método permite executar uma instalação autônoma usando a linha de comando do Windows.

O diagrama a seguir ilustra como instalar o aplicativo:

A tabela a seguir lista os tópicos que descrevem as tarefas para instalar o CA ARCserve Central Host-Based VM Backup:

Tarefa	Consultar o tópico
Executar as tarefas de pré-requisito da instalação e revisar as considerações sobre a instalação antes de instalar o aplicativo.	Tarefas essenciais da instalação (na página 17)
Executar uma instalação padrão usando o Assistente de Instalação.	Instalar o CA ARCserve Central Host-Based VM Backup (na página 19)
Executar uma instalação silenciosa usando a linha de comando do Windows.	Instalar o CA ARCserve Central Host-Based VM Backup de modo silencioso (na página 21)

Para obter mais informações sobre a atualização de vários componentes do sistema operacional Windows após instalar o aplicativo, consulte a seção Aplicando as práticas recomendadas no Guia do Usuário do CA ARCserve Central Host-Based VM Backup.

Tarefas essenciais da instalação

Antes de instalar o aplicativo, conclua as seguintes tarefas de pré-requisito e revise as considerações de instalação:

Tarefas de pré-requisito

- Examine as Notas da versão. As Notas da Versão contêm uma descrição de requisitos do sistema, sistemas operacionais suportados e uma lista de problemas conhecidos nesta versão do aplicativo.
- Verifique se o sistema atende aos requisitos de software e hardware que são necessários para instalar o aplicativo.
- Verifique se é possível ativar o rastreamento de bloco alterado e se ele está ativado nas máquinas virtuais que estiver protegendo.

  Observação: para obter mais informações sobre o rastreamento do bloco alterado, consulte o seguinte documento da base de dados de conhecimento no site da VMware:

  http://kb.vmware.com/kb/1020128
- Verifique se sua conta do Windows tem privilégios de administrador ou equivalente para instalar o software nos computadores em que planeja instalar o CA ARCserve Central Host-Based VM Backup.
- Verifique se a sua conta vCenter ou ESX Server tem privilégios administrativos do VMware ou do Windows. Atribua a conta à função Licença global no sistema vCenter Server ou no sistema ESX Server para permitir que as operações do VDDK sejam concluídas com êxito.

- Verifique se você tem em mãos os nomes de usuário e senhas dos computadores em que você está instalando o aplicativo.
- Verifique se o CA ARCserve D2D está instalado no sistema proxy de backup que protege as máquinas virtuais no seu ambiente de produção.
- Se desejar fazer a restauração granular do backup da VM, verifique se as credenciais internas ou do administrador de domínio de qualquer usuário com privilégios administrativos foram fornecidas para logon no sistema operacional convidado da máquina virtual.
- O CA ARCserve Central Applications permite instalar e atualizar o CA ARCserve D2D e atualizar a versão anterior para a versão mais recente em nós remotos usando o utilitário de implantação. Para fazer o backup de dados nos nós remotos usando a versão mais recente do CA ARCserve D2D, você deve obter a versão mais recente das licenças do CA ARCserve D2D e aplicar as licenças nos nós. Se você não aplicar as licenças em 31 dias a partir da data em que instalou ou atualizou nos nós, o CA ARCserve D2D irá parar de funcionar.

Considerações sobre a instalação

Antes de instalar o CA ARCserve Central Host-Based VM Backup, revise as seguintes considerações de instalação:

- O pacote de instalação do CA ARCserve Central Applications instala um módulo chamado Servidor do CA ARCserve Central Applications. O servidor é um módulo comum a todos os aplicativos. O módulo contém o serviço web, os binários e configurações que permitem que o aplicativo se comunique com os outros.

  Ao instalar o aplicativo, o pacote de instalação instala o módulo do Servidor do CA ARCserve Central Applications antes de instalar os componentes do produto. Se for necessário aplicar um patch ao aplicativo, ele atualizará o módulo antes de atualizar os componentes do produto.
- Depois da instalação do CA ARCserve Central Host-Based VM Backup, faça download e instale o API do VMware VIX versão 1.11 no sistema proxy de backup e no computador usado para executar verificações antecipadas. O VMware VIX é usado para executar restaurações em nível de arquivo e em nível de aplicativo a partir do backup.

  Observação: para VIX API 1.11, é necessário que todas as máquinas virtuais sejam atualizadas com as mais recentes ferramentas do VMware.
- O CA ARCserve D2D instala o VDDK (VMware Virtual Disk Development Kit) em todos os computadores onde o CA ARCserve D2D foi instalado. Não é necessário baixar e instalar o VDDK nos sistemas proxy de backup.

  Se você deseja usar uma versão diferente do VDDK, faça download e instale o VDDK e, em seguida, modifique o valor do registro VDDKDirectory localizado em HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE D2D para a pasta de instalação onde o novo VDDK está instalado.

  O local padrão para o VDDK é o seguinte:

- **Sistema operacional X64**

  `c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit`

  Observação: descompacte o arquivo VDDK64.zip no diretório de instalação do VDDK para a pasta VDDK64.

  Por exemplo, c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit\VDDK64

- **Sistema operacional X86**

  `c:\Program Files\VMware\VMware Virtual Disk Development Kit`

- É necessário uma instalação local do CA ARCserve D2D para a realização de certas operações de restauração. Para obter mais informações, consulte o tópico Considerações sobre a restauração. (na página 105) As licenças para o CA ARCserve D2D estão incluídas no CA ARCserve Central Host-Based VM Backup. Para obter os arquivos de instalação do produto, visite site de suporte da CA.
- A compatibilidade virtual para o mapeamento de dispositivos brutos é suportada, mas não a compatibilidade física.

Instalar o CA ARCserve Central Host-Based VM Backup

O Assistente de instalação ajuda a orientá-lo durante todo o processo de instalação de um ou mais CA ARCserve Central Applications.

Observação: antes de instalar o aplicativo, consulte o arquivo Notas da versão e verifique se todas as tarefas descritas em Tarefas de pré-requisito foram concluídas.

Para instalar o CA ARCserve Central Host-Based VM Backup

1. Baixe o pacote de instalação do CA ARCserve Central Applications para o computador no qual você deseja instalar o aplicativo e clique duas vezes no Arquivo de instalação.

   O pacote de instalação extrai seu conteúdo para o computador e, em seguida, a caixa de diálogo Componentes essenciais é aberta.

2. Clique em Instalar na caixa de diálogo Componentes essenciais.

   Observação: a caixa de diálogo Componentes essenciais será exibida somente se o programa de instalação não detectar os componentes essenciais instalados no computador.

   Depois que o programa de instalação instalar os componentes essenciais, a caixa de diálogo do Contrato de licença é aberta.

3. Preencha os campos necessários da caixa de diálogo Contrato de licença e clique em Avançar.

   A caixa de diálogo Configuração é aberta.

4. Na caixa de diálogo de Configuração, preencha o seguinte:

   - **Componentes -** especifique os aplicativos que você deseja instalar.

     Observação: se instalar esse aplicativo usando o conjunto do pacote de instalação, você poderá instalar vários aplicativos.

   - **Local -** aceite o local padrão da instalação ou clique em Procurar para especificar um local de instalação alternativo. O diretório padrão é o seguinte:

     `C:\Arquivos de programas\CA\ARCserve Central Applications\BIN`

   - **Informações do disco -** verifique se o disco rígido tem espaço livre suficiente para instalar os aplicativos.

   - **Nome do administrador do Windows -** especifique o nome de usuário da conta de administrador do Windows usando a seguinte sintaxe:

     `Domínio\Nome do usuário`

   - **Senha -** especifique a senha da conta do usuário.

   - **Especificar o número da porta -** especifique o número de porta que deseja usar para se comunicar com a interface do usuário baseada na web. Como prática recomendada, você deve aceitar o número de porta padrão. O número da porta padrão é o seguinte:

     `8015`

     Observação: se desejar especificar um outro número de porta, os números de porta disponíveis vão de 1024 a 65535. Para que você especifique um outro número de porta, verifique se o número de porta especificado está livre e disponível para uso. A instalação impede que você instale o aplicativo usando uma porta que não esteja disponível para uso.

   - **Usar HTTPS para a comunicação web** - especifique usar a comunicação HTTPS para a transmissão de dados. Essa opção não vem selecionada por padrão.

     Observação: a comunicação HTTPS (segura) fornece um nível maior de segurança do que a comunicação HTTP. O HTTPS é o protocolo de comunicação recomendado se você transmite informações confidenciais na rede.

   - **Permitir que o programa de instalação registre como exceções os serviços/programas do CA ARCserve Central Applications no Firewall do Windows -** verifique se a caixa de seleção para essa opção está marcada. As exceções do firewall são necessárias para configurar e gerenciar o CA ARCserve Central Applications por meio de computadores remotos.

     Observação: para usuários locais, não é preciso registrar as exceções do firewall.

   Clique em Avançar.

   Depois que o processo de instalação é concluído, o relatório de instalação é aberto.

5. A caixa de diálogo Relatório de instalação resume a instalação. Se deseja verificar se há atualizações para o aplicativo agora, clique em Verificar se há atualizações e clique em Concluir.

O aplicativo está instalado.

Instalar o CA ARCserve Central Host-Based VM Backup de modo silencioso

O CA ARCserve Central Applications permite instalar o CA ARCserve Central Host-Based VM Backup de modo silencioso. O processo de instalação silenciosa elimina a necessidade de interação com o usuário. As etapas a seguir descrevem como instalar o aplicativo usando a linha de comando do Windows.

Para instalar o CA ARCserve Central Host-Based VM Backup silenciosamente

1. Abra a linha de comando do Windows no computador onde deseja iniciar o processo de instalação silenciosa.
2. Faça download do pacote de instalação de auto-extração do CA ARCserve Central Applications para o computador.

   Inicie o processo de instalação silenciosa usando a seguinte sintaxe da linha de comando:

   ```
   "CA ARCserve Central Applications Setup.exe" /s /v"/q -Path:<INSTALLDIR>
   -Port:<PORT> -U:<UserName> -P:<Password> -Products:<ProductList>"
   ```

   Utilização:

   s

   Permite executar o pacote de arquivo executável no modo silencioso.

   v

   Permite especificar outras opções de linha de comando.

   q

   Permite instalar o aplicativo no modo silencioso.

   -Path:<INSTALLDIR>

   (Opcional) Permite especificar o caminho de instalação de destino.

   Exemplo:

   ```
   -Path:\"C:\Arquivos de Programas\CA\ARCserve Central Applications\"
   ```

   Observação: se o valor de INSTALLDIR tiver um espaço, coloque o caminho entre barras invertidas e aspas. Além disso, o caminho não pode terminar com um caractere de barra invertida.

-Port:<PORT>

(Opcional) Permite especificar o número da porta para comunicação.

Exemplo:

```
-Porta:8015
```

-U:<UserName>

Permite especificar o nome de usuário a ser usado para instalar e executar o aplicativo.

Observação: o nome de usuário deve ser uma conta administrativa ou uma conta com privilégios administrativos.

-P:<Password>

Permite especificar a senha para o nome de usuário.

-Products:<ProductList>

(Opcional) Permite especificar uma instalação do CA ARCserve Central Applications de modo silencioso. Se você não especificar um valor para o argumento, o processo de instalação silenciosa instalará todos os componentes do CA ARCserve Central Applications.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

Todos os aplicativos CA ARCserve Central Applications

TODOS

Observação: os exemplos a seguir descrevem a sintaxe necessária para instalar um, dois, três ou todos os aplicativos CA ARCserve Central Applications silenciosamente:

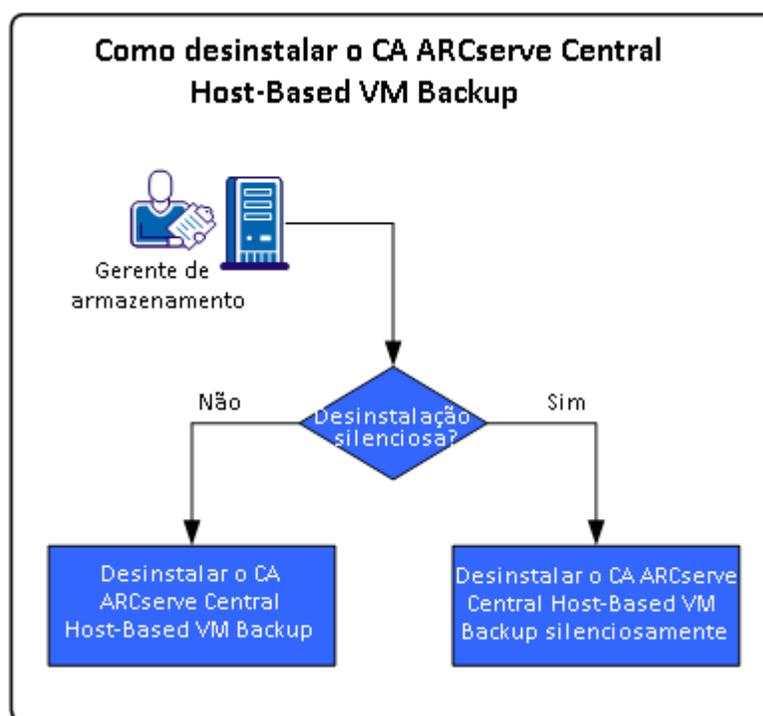
```
-Products:<CMX64>
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:<ALL>
```

O aplicativo foi instalado de modo silencioso.

Como desinstalar o CA ARCserve Central Host-Based VM Backup

Você pode instalar o CA ARCserve Central Host-Based VM Backup usando os seguintes métodos:

- Desinstalação padrão - este método usa o Painel de Controle do Windows para desinstalar o aplicativo.
- Desinstalação silenciosa - este método permite executar uma desinstalação autônoma usando a linha de comando do Windows.

O diagrama a seguir ilustra como desinstalar o aplicativo:

Tarefa	Consultar o tópico
Executar uma desinstalação padrão usando o Painel de Controle do Windows.	Desinstalar o CA ARCserve Central Host-Based VM Backup (na página 24)
Executar uma desinstalação silenciosa usando a linha de comando do Windows.	Desinstalar o CA ARCserve Central Host-Based VM Backup de modo silencioso (na página 25)

Para obter mais informações sobre a atualização de vários componentes do sistema operacional Windows após desinstalar o aplicativo, consulte a seção Aplicando as práticas recomendadas no Guia do Usuário do CA ARCserve Central Host-Based VM Backup.

Desinstalar o CA ARCserve Central Host-Based VM Backup

É possível desinstalar o aplicativo usando Programas e Recursos, localizado no Painel de Controle do Windows.

Para desinstalar o CA ARCserve Central Host-Based VM Backup

1. No menu Iniciar do Windows, clique em Iniciar e em Painel de controle.

   O Painel de controle do Windows é aberto.

2. No Painel de controle do Windows, clique na lista suspensa próxima a Exibir por e, em seguida, clique em Ícones grandes ou Ícones pequenos.

   Os ícones dos aplicativos no Painel de controle do Windows aparecem em um layout de grade.

3. Clique em Programas e Recursos.

   A janela Desinstalar ou alterar um programa é aberta.

4. Localizar e clique no aplicativo que deseja desinstalar.

   Clique com o botão direito do mouse no aplicativo e clique em Desinstalar no menu pop-up.

   Siga as instruções na tela para desinstalar o aplicativo.

O aplicativo será desinstalado.

Desinstalar o CA ARCserve Central Host-Based VM Backup de modo silencioso

O CA ARCserve Central Applications permite desinstalar o CA ARCserve Central Host-Based VM Backup de modo silencioso. O processo de desinstalação silenciosa elimina a necessidade de interação com o usuário. As etapas a seguir descrevem como desinstalar o aplicativo usando a linha de comando do Windows.

Para desinstalar o CA ARCserve Central Host-Based VM Backup de modo silencioso

1. Efetue logon no computador de onde deseja desinstalar o aplicativo.

   Observação: é necessário efetuar logon usando uma conta administrativa ou uma conta com privilégios administrativos.

2. Abra a linha de comando do Windows e execute o seguinte comando para iniciar o processo de desinstalação silenciosa:

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /p <ProductCode>
   ```

   Ou

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /ALL
   ```

   Exemplo: a sintaxe a seguir permite desinstalar o CA ARCserve Central Host-Based VM Backup de modo silencioso.

   ```
   "%ProgramFiles%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}
   ```

Utilização:

<INSTALLDIR>

Permite especificar o diretório no qual o aplicativo está instalado.

Observação: execute a sintaxe que corresponde à arquitetura do sistema operacional do computador.

<ProductCode>

Permite especificar o aplicativo a ser desinstalado silenciosamente.

Observação: o processo de desinstalação silenciosa permite instalar um ou mais aplicativos CA ARCserve Central Applications. Use os seguintes códigos de produtos para desinstalar o CA ARCserve Central Applications de modo silencioso:

CA ARCserve Central Host-Based VM Backup

{CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

CA ARCserve Central Protection Manager

{CAED05FE-D895-4FD5-B964-001928BD2D62}

CA ARCserve Central Reporting

{CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

CA ARCserve Central Virtual Standby

{CAED4835-964B-484B-A395-E2DF12E6F73D}

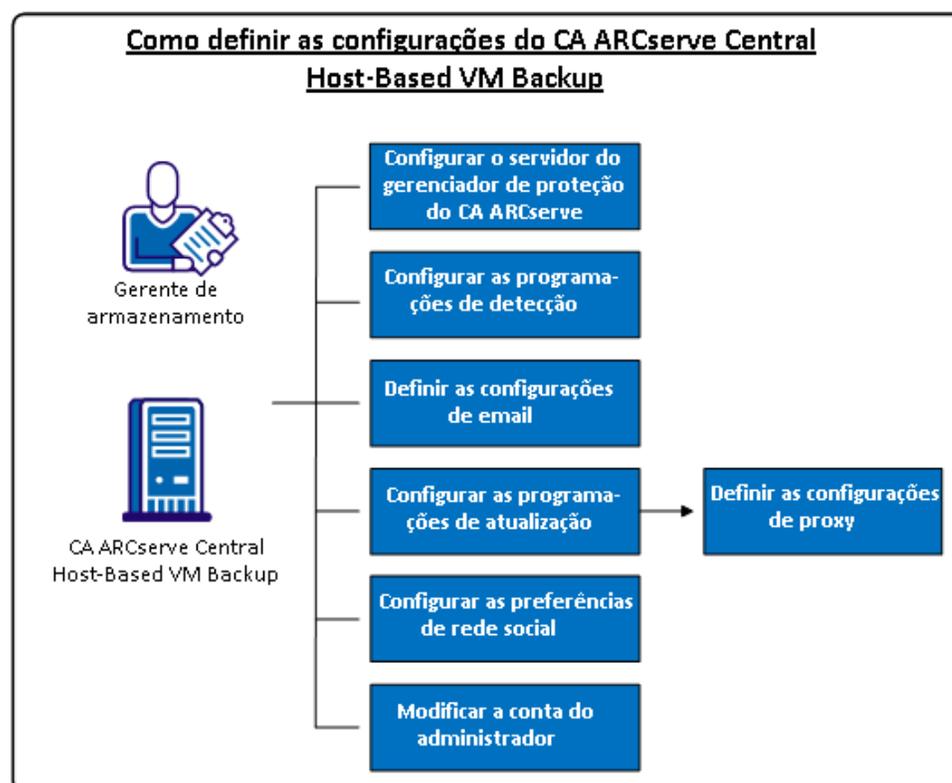
O aplicativo é desinstalado de modo silencioso.

Como configurar o CA ARCserve Central Host-Based VM Backup Proteger nós do CA ARCserve D2D

O aplicativo permite especificar as configurações para os alertas de email e as programações e como atualizar sua instalação do CA ARCserve Central Host-Based VM Backup.

Antes de começar a especificar as definições de configuração, é necessário primeiro instalar o CA ARCserve D2D no servidor que executa as tarefas de backup. Esse elemento, ou o servidor proxy, pode ser um único computador ou várias máquinas, dependendo das suas necessidades. Para obter instruções, consulte o tópico Instalar o CA ARCserve D2D, extraído do Guia do Usuário do CA ARCserve D2D.

É possível instalar o CA ARCserve Central Host-Based VM Backup no mesmo computador ou em um computador separado. O procedimento de instalação é auxiliado por um assistente para maior facilidade. Para obter mais informações, consulte Instalar o CA ARCserve Central Host-Based VM Backup.

A ilustração a seguir descreve os tipos de configurações que você pode definir para o aplicativo:

Este cenário descreve os seguintes tópicos:

- Configurar o servidor do CA ARCserve Central Protection Manager (na página 28)

Configurar o Servidor do CA ARCserve Central Protection Manager

Configurar o servidor do CA ARCserve Central Protection Manager permite alterar as configurações atuais no CA ARCserve Central Host-Based VM Backup para as configurações do servidor do CA ARCserve Central Protection Manager. Quando as configurações são definidas, é possível visualizar a informação de alerta de email dos nós descobertos do Host-Based VM Backup do CA ARCserve Central Reporting.

Siga estas etapas:

1. Efetue logon no servidor do CA ARCserve Central Host-Based VM Backup e clique em Configuração na barra de navegação.

   A tela Configuração é exibida.

2. No Painel de configuração, clique em Configuração do CA ARCserve Central Protection Manager.

3. Preencha os seguintes campos:

   - **Servidor do CA ARCserve Central Protection Manager**

     Observação: com o CA ARCserve Central Protection Manager e o CA ARCserve Central Host-Based VM Backup instalados, os seguintes campos serão padrão para o servidor local do CA ARCserve Central Protection Manager. Se o CA ARCserve Central Protection Manager não estiver instalado, o campo permanece em branco e será necessário configurá-lo manualmente. É possível exibir as informações de alerta dos nós detectados do CA ARCserve Central Reporting.

- **Nome da máquina**--o nome de host do computador em que o CA ARCserve Central Protection Manager está instalado.
- **Nome de usuário** -- o nome de usuário necessário para efetuar logon no computador onde o CA ARCserve Central Protection Manager está instalado.
- **Senha**--a senha do usuário.
- **Porta**--o número de porta a ser usado para se comunicar com o serviço web do CA ARCserve Central Protection Manager.
- **HTTPS** -- esta opção é marcada ou desmarcada com base na conexão configurada no servidor do CA ARCserve Central Protection Manager.

- **Detectar a porta e o protocolo automaticamente** -- permite obter a porta e o protocolo do banco de dados do Gerenciador de Proteção do CA ARCserve Central Protection Manager e preenche os campos anteriores.

  Observação: essa opção será ativada apenas se o acesso ao registro remoto do servidor do CA ARCserve Central Protection Manager for permitido.

  Para verificar se o registro remoto é permitido ou não, execute as seguintes etapas:

  1. Vá para o servidor do CA ARCserve Central Protection Manager onde o CA ARCserve Central Protection Manager está instalado.
  2. Navegue para services.msc e verifique se o serviço "Registro Remoto" foi iniciado.
  3. Defina para "Automático".

- **Teste -** permite verificar se as informações de acesso do CA ARCserve Central Protection Manager estão corretas.

4. Clique em Salvar.

Configurar programações de detecção

É possível configurar a programação de detecção para nós de forma repetitiva e em um horário programado. Por padrão, a Configuração da detecção está desativada. Para ativar a configuração, clique na opção Ativar para especificar o tipo de método de repetição desejado e um horário programado para que a detecção do nó se inicie. É possível especificar os seguintes parâmetros para configurar a programação de detecção:

- **Cada quantidade de dias -** permite repetir este método pelo número de dias especificado. (Padrão)
- **Cada dia selecionado da semana -** permite repetir este método nos dias especificados. Segunda-feira, Terça-feira, Quarta-feira, Quinta-feira e Sexta-feira são o padrão para os dias da semana.
- **Cada dia selecionado do mês -** permite repetir este método no dia especificado do mês. 1 é a opção padrão para o dia do mês.

Uma lista do vCenter/ESX é exibida ao visualizar a configuração de uma programação para detectar nós.

Definir a configuração de email e alerta

É possível especificar configurações de email e alerta para uso com seu aplicativo, de modo a enviar automaticamente alertas sob as condições determinadas.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, clique em Configuração para abrir a tela Configuração.

2. No painel Configuração, clique em Configuração de email e alerta para abrir as opções de Configuração de email e alerta.

3. Preencha os seguintes campos:
   - **Serviço** - especifique o tipo de serviço de email na lista suspensa. (Google Mail, Yahoo Mail, Live Mail ou Outro).
   - **Servidor de email**--especifique o nome do host do servidor SMTP que o CA ARCserve Central Applications deve usar para enviar email.
   - **Requer autenticação**-selecione essa opção quando o servidor de email especificado exigir autenticação. O nome da conta e a senha serão necessários.
   - **Assunto**--especifique um assunto de email padrão.
   - **De**--especifique o endereço de email para o qual o email está sendo enviado.
   - **Destinatário**--especifique um ou mais endereços de email, separados por um ponto e vírgula (;), para os quais o email será enviado.
   - **Usar SSL** - selecione essa opção se o servidor de email especificado exigir uma conexão segura (SSL).
   - **Enviar STARTTLS** - selecione essa opção se o servidor de email especificado exigir o comando STARTTLS.
   - **Usar formato HTML** - permite enviar mensagens de email no formato HTML. (selecionado por padrão)
   - **Ativar configurações de proxy** - selecione essa opção se houver um servidor proxy. Em seguida, especifique as configurações do servidor proxy.
4. Clique em Testar email para verificar se as definições das configurações de email estão corretas.
5. (Opcional) Na seção Enviar alertas por email, clique nos nós detectados para permitir que o aplicativo envie mensagens de alerta por email quando novos nós forem detectados.
6. Clique em Salvar.

   Observação: você pode clicar em Redefinir para reverter aos valores salvos anteriormente ou clicar em Excluir para excluir as configurações salvas. Excluir as configurações de email e alerta evita que você receba mensagens de alerta por email.

A configuração de email é aplicada.

Configurar programações de atualização

O aplicativo permite configurar uma programação para fazer download automaticamente de atualizações do produto de um Servidor da CA ou de um servidor de armazenamento temporário de software local.

Siga estas etapas:

1. Efetue logon no aplicativo.
2. Clique em Configuração na barra de navegação para abrir a tela Configuração.
3. No painel Configuração, clique em Atualizar configuração.

   As opções de configuração de atualização são exibidas.
4. Selecione um servidor de download.
   - **CA Server** - clique em Configurações de proxy para as seguintes opções:
     - **Usar configurações de proxy do navegador -** permite usar as credenciais fornecidas para as configurações de proxy do navegador.

       Observação: a opção Usar configurações de proxy do navegador afeta o Internet Explorer e o Chrome.
     - **Configurar definições de proxy** - especifique o Endereço IP ou o Nome do host do servidor proxy e o número de porta. Se o servidor especificado exigir autenticação, clique em O servidor proxy exige autenticação e forneça as credenciais.

       Clique em OK para voltar à Atualizar configuração.
   - **Servidor de armazenamento temporário -** se você selecionar essa opção, clique em Adicionar Servidor para adicionar um servidor de armazenamento temporário na lista. Digite o nome de host e o número da porta e clique em OK.

     Se forem especificados vários servidores de armazenamento temporário, o aplicativo tentará usar o primeiro servidor da lista. Se a conexão for bem-sucedida, os demais servidores relacionados não são usados para armazenamento temporário.
5. (Opcional) Clique em Testar conexão para verificar a conexão de servidor e aguarde até que o teste seja concluído.
6. (Opcional) Clique em Verificar atualizações automaticamente e especifique o dia e a hora. Você pode especificar uma programação diária ou semanal.

Clique em Salvar para aplicar a configuração atualizada.

Definir configurações de proxy

O CA ARCserve Central Applications permite especificar um servidor proxy para se comunicar com o suporte da CA a fim de verificar e fazer download das atualizações disponíveis. Para ativar este recurso, é necessário especificar o servidor proxy que deseja que se comunique em nome do servidor do CA ARCserve Central Applications.

Siga estas etapas:

1. Efetue logon no aplicativo e clique em Configuração na barra de navegação.

   A opção Configuração é exibida.

2. Clique em Atualizar configuração.

   As opções de configuração de atualização são exibidas.

3. Clique em Configurações de proxy.

   A caixa de diálogo Configurações de proxy é aberta.

4. Clique em uma das seguintes opções:
   - **Usar configurações de proxy do navegador --**permite que o aplicativo detecte e use as mesmas configurações de proxy que são aplicadas para o navegador para se conectar ao servidor da CA Technologies para atualizar as informações.

     Observação: esse comportamento se aplica somente aos navegadores Internet Explorer e Chrome.
   - **Definir configurações de proxy**--permite definir um servidor alternativo que o aplicativo usará para se comunicar com o suporte da CA para verificar se há atualizações. O servidor alternativo (proxy) pode ajudar a garantir a segurança, melhorar o desempenho e garantir o controle administrativo.

     Preencha os seguintes campos:
     - **Servidor proxy--** especifique o nome do host ou o endereço IP do servidor proxy.
     - **Porta--**especifique o número de porta que o servidor proxy usará para se comunicar com o site de suporte da CA.
     - **(Opcional) o servidor proxy requer autenticação--** se as credenciais de logon do servidor proxy não forem as mesmas do CA ARCserve Central Applications, clique na caixa de seleção próxima ao Servidor proxy requer autenticação, e especifique o nome de usuário e a senha necessárias para efetuar logon no servidor proxy.

       Observação: use o seguinte formato para especificar o nome de usuário: <nome de domínio>/<nome de usuário>.

   Clique em OK.

As configurações de proxy são definidas

Observação: para ajudar a garantir que o CA ARCserve Central Host-Based VM Backup possa implantar diretivas aos nós e proteger os nós do CA ARCserve D2D, verifique se o servidor do Host-Based VM Backup e o servidor proxy podem se comunicar uns com os outros usando seus nomes de host. Siga as seguintes etapas:

1. No servidor do CA ARCserve Central Host-Based VM Backup execute o comando ping no servidor proxy usando seu nome de host.
2. No servidor proxy, execute o comando ping no servidor do CA ARCserve Central Host-Based VM Backup usando o nome do host do servidor.

Configurando preferências de redes sociais

O CA ARCserve Central Applications permite gerenciar as ferramentas de rede social para ajudá-lo a gerenciar o aplicativo. Você pode gerar novos feeds, especificar links para sites de redes sociais populares e selecionar sites de fonte de vídeos.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, clique em Configuração para abrir a tela Configuração.

2. No painel Configuração, clique em Configuração de preferências para abrir as opções de Preferências.

3. Especifique as opções necessárias:

   - **Feed de notícias -** permite que o aplicativo exiba feeds RSS de notícias relacionadas ao CA ARCserve Central Applications e ao CA ARCserve D2D e informações do produto (do Expert Advice Center). Os feeds são exibidos na página inicial.
   - **Rede social -** permite que o aplicativo exiba ícones na página inicial para acesso ao Twitter e ao Facebook para sites de redes sociais relacionados ao CA ARCserve Central Applications e ao CA ARCserve D2D .
   - **Vídeos -** permite selecionar o tipo de vídeo para exibição dos produtos do CA ARCserve Central Applications e CA ARCserve D2D. (A opção padrão é Usar vídeos do YouTube.)

   Clique em Salvar.

   As opções de Rede social são aplicadas

4. Na barra de navegação, clique em Página Inicial.

   A Página inicial é exibida.

5. Atualize a janela do navegador.

   As opções de Rede social são aplicadas.

Modificar a conta do administrador

O CA ARCserve Central Applications permite modificar o nome de usuário, senha, ou ambos da conta do administrador depois de instalar o aplicativo. Esta conta de administrador somente é usada para exibição do nome de usuário padrão na tela de logon.

Observação: o nome de usuário especificado deve ser uma conta administrativa do Windows ou uma conta que tenha privilégios administrativos do Windows.

Siga estas etapas:

1. Efetue logon no aplicativo e clique em Configuração na barra de navegação.

   A opção Configuração é exibida.

2. Clique em Conta de administrador
3. A configuração da conta do administrador é exibida.
4. Atualize os seguintes campos, conforme necessário:
   - Nome de usuário
   - Senha

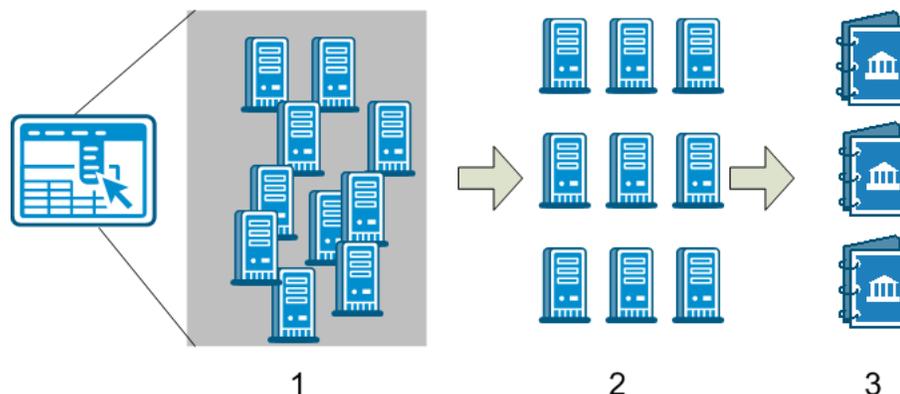
   Clique em Salvar

A conta do administrador é modificada.

Capítulo 3: Usando o CA ARCserve Central Host-Based VM Backup

Esta seção contém os seguintes tópicos:

Como configurar o ambiente de produção

Proteger o ambiente de máquina virtual requer algumas atividades básicas:

1. Adicionar os nós ao CA ARCserve Central Host-Based VM Backup. É possível importar todas as máquinas virtuais hospedadas por um servidor ESX ou vCenter.
2. Agrupar os nós para facilitar seu gerenciamento. Por exemplo, é possível agrupar nós por função de negócios ou por aplicativos instalados.
3. Criar diretivas de backup e atribuir uma diretiva a um nó. Todos os nós são incluídos no backup de acordo com a diretiva definida.

Como usar a página inicial do CA ARCserve Central Host-Based VM Backup

Quando o CA ARCserve Central Host-Based VM Backup é iniciado, uma página inicial é aberta no navegador. Na página inicial, é possível executar as seguintes tarefas:

- **Navegação à esquerda**:
  - **Nó** - a tela Nó permite exibir o ambiente de máquina virtual de acordo com os grupos de nós, aplicativos instalados e Diretiva do vSphere atribuída.
  - **Diretivas** - a tela Diretivas do vSphere permite criar, editar e atribuir diretivas de backup a todos os nós do ambiente.
  - **Configuração** - a tela Configuração permite especificar os alertas por email e a programação de atualização automática para o aplicativo.
  - **Exibir logs** - a tela Exibir logs permite encontrar ocorrências específicas: Informações, Erros ou Avisos.
  - **Adicionar nova guia** - você pode adicionar manualmente o nome e a URL de qualquer site que deseja monitorar.
  - **Suporte da CA** - permite obter acesso a vários sites de suporte e de rede social, incluindo Facebook e Twitter.

Fazer logon em Nós do CA ARCserve D2D

Na página inicial do Host-Based VM Backup, é possível efetuar logon nos nós do CA ARCserve D2D.

Para fazer logon em nós do CA ARCserve D2D

1. Abra o aplicativo e clique em Nós na Barra de navegação.

   A tela Nó é exibida.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Procure e clique no nó que deseja efetuar logon e, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   Uma versão CA ARCserve Central Host-Based VM Backup do CA ARCserve D2D é exibida.

   Observação: se uma nova janela do navegador não for aberta, verifique se as opções de pop-up de seu navegador permitem todos os pop-ups ou pop-ups somente para este site.

Você está conectado ao nó do CA ARCserve D2D.

Observação: a primeira vez que efetuar logon no nó do CA ARCserve D2D, uma página HTML pode se abrir exibindo uma mensagem de aviso. Isso pode ocorrer quando estiver usando o Internet Explorer. Para corrigir esse comportamento, feche o Internet Explorer e repita a etapa 3. Assim, será possível fazer logon no nó do CA ARCserve D2D com êxito.

Como gerenciar tarefas de nós do CA ARCserve Central Host-Based VM Backup

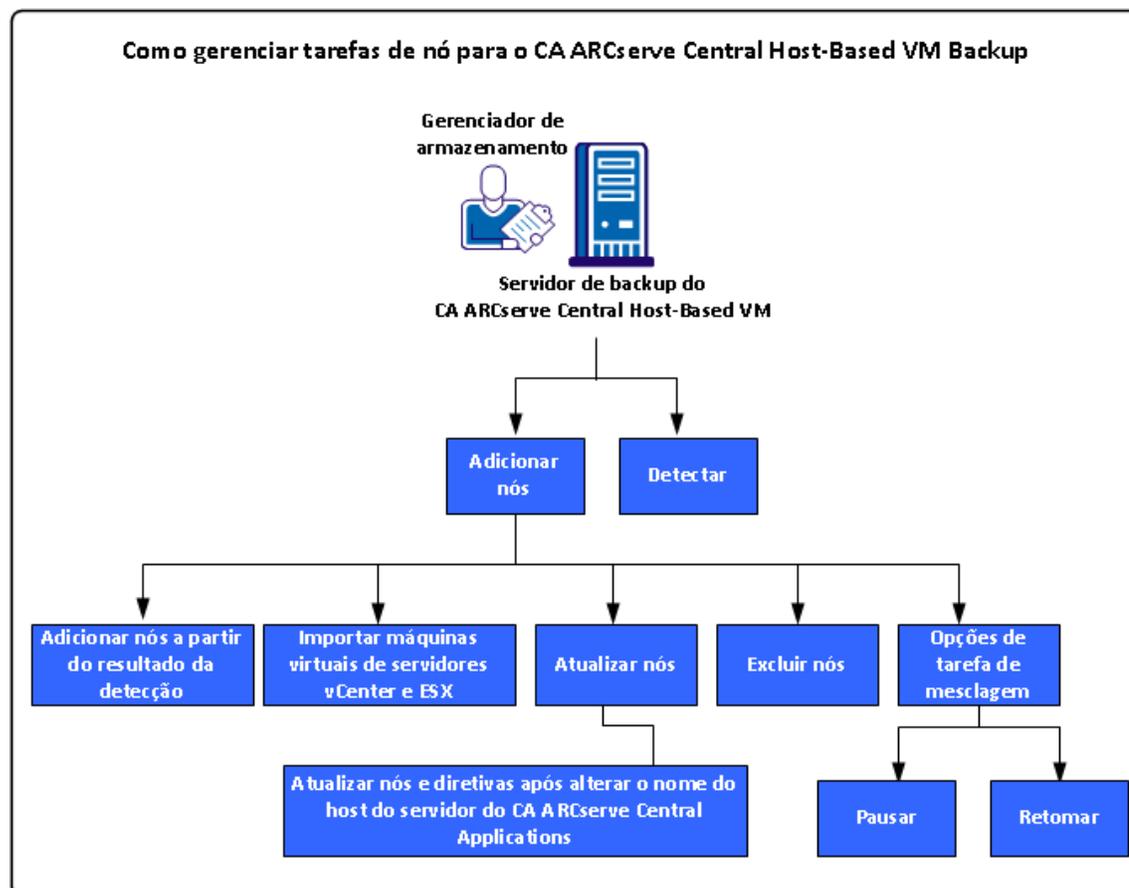
Este cenário explica como os Gerentes de Armazenamento podem gerenciar os nós. Por exemplo, adicionar ou detectar nós, atribuir nós a grupos de nós e atualizar ou excluir nós da tela Nó.

A tabela a seguir descreve os itens que são exibidos na tela Nó:

Nome da coluna	Descrição
Nome do nó	Exibe o nome do nó. **Observação**: alguns nós listados podem não estar ativados para você selecionar. O motivo é que o nó não pode ser detectado pelo servidor. Por exemplo, ele pode ser excluído do servidor.

Nome da coluna	Descrição
Diretiva	Exibe o nome da diretiva e o status de implantação de diretiva.
Nome da máquina virtual	Exibe o nome da máquina virtual.
vCenter/ESX	Exibe os detalhes do servidor que ajudam a detectar máquinas virtuais.
Tarefa (na página 69)	Exibe o status da tarefa de backup e vincula ao Monitor de status de backup (na página 70) para obter mais detalhes.
Status	Exibe o status do nó: ■ = Erro/Falha ■ = Aviso ■ = Êxito Se você passar o mouse sobre o ícone, uma tabela pop-up Resumo de status do nó será exibida com os resultados para as seguintes categorias: ■ Último backup - exibe o tipo, a data e hora, e o status do backup. ■ Pontos de recuperação - exibe a quantidade de pontos de recuperação do servidor monitorado. ■ Capacidade do destino - exibe a quantidade de espaço livre disponível no destino de backup.
Resultado do último backup	Exibe o status da última tarefa de backup.
Hora do último backup	Exibe a data e hora da última tarefa de backup.

<table>
<tr><th>Nome da coluna</th><th>Descrição</th></tr>
<tr><td>Status de PFC</td><td>Exibe o status da verificação prévia de suas tarefas de backup:
= Erro/Falha
= Aviso
= Êxito
O ícone determina se uma tarefa de backup pode ser executada ou não para o nó específico.
Se você passar o mouse sobre o ícone, uma tabela pop-up Verificação será exibida com os resultados para as seguintes categorias:
CBT (Changed Block Tracking - Rastreamento do Bloco Alterado) - exibe o resultado de CBT para o backup.
VMware Tools - exibe se a ferramenta de VMware está instalada ou não.
Disco - exibe o status do disco.
Estado da energia - exibe se a máquina virtual está ligada ou desligada.
Credenciais - exibe o status das credenciais do usuário.
Aplicativos - exibe o status de instalação do aplicativo no nó.
Para obter mais detalhes, consulte o tópico Executar verificações prévias para suas tarefas de backup (na página 58).</td></tr>
<tr><td>Aplicativos</td><td>Exibe o aplicativo ao qual o nó está associado.</td></tr>
<tr><td>OS</td><td>Exibe o sistema operacional ao qual o nó está associado.</td></tr>
<tr><td>Descrição</td><td>Exibe uma descrição do nó.</td></tr>
</table>

O diagrama a seguir ilustra as tarefas que você pode executar nos Nós.

Este cenário descreve as opções que podem ser usadas ao adicionar ou atualizar os nós:

- Detectar (na página 43)
- Adicionar nós (na página 44)
  - Adicionar nós a partir do resultado da detecção automática (na página 45)
  - Importar máquinas virtuais de servidores vCenter/ESX (na página 46)
- Atualizar nós (na página 47)
  - Atualizar nós e diretivas depois de alterar o nome do host no servidor do CA ARCserve Central Applications (na página 48)
- Excluir nós (na página 48)
- Opções da tarefa de mesclagem (na página 49)
  - Pausar uma tarefa de mesclagem em um nó (na página 49)
  - Retomar uma tarefa de mesclagem em um nó (na página 50)

Detectar nós do CA ARCserve Central Host-Based VM Backup

O CA ARCserve Central Host-Based VM Backup permite detectar nós automaticamente adicionando os sistemas vCenter Server e ESX Server ao seu ambiente. Ao adicioná-los, o aplicativo poderá detectar máquinas virtuais que eles hospedam automaticamente.

Importante: O processo de detecção de nós requer que você especifique o nome do host ou o endereço IP do vCenter Server ou do sistema ESX Server. Essas informações permitem que o processo de detecção encontre máquinas virtuais conectadas ao vCenter Server e aos sistemas ESX Server. Quando você achar necessário modificar o nome do host ou o endereço IP de um sistema vCenter Server ou ESX Server, repita as etapas descritas neste tópico e reimplante a diretiva de backup para criar um novo conjunto de backup com o nome do host ou o endereço IP atualizado.

Siga estas etapas:

1. Efetue logon no aplicativo e clique em Nó na barra de navegação para abrir a tela Nó.
2. Clique em Detectar na barra de ferramentas para abrir a caixa de diálogo Detectar nós do vCenter/ESX Server.
3. Na caixa de diálogo Detectar nós do vCenter/ESX Server, preencha os seguintes campos:
   - Host do vCenter/ESX
   - Nome de usuário

     Observação: a conta especificada deve ser de uma conta com privilégios administrativos no sistema ESX Server ou vCenter Server.
   - Senha
   - Porta

   Clique em Adicionar.

   Observação: repita essa etapa para adicionar mais sistemas vCenter/ESX Server.
4. Clique em Detectar para iniciar o processo de detecção.

   O Monitor de detecção é exibido, mostrando o andamento da detecção.
5. Quando o processo de detecção for concluído, uma mensagem de confirmação será exibida: Deseja continuar a adicionar nós a partir do resultado da detecção?

   Clique em Sim e a tela Adicionar nós a partir do resultado da detecção será exibida, ou clique em Não se tiver mais hipervisores para adicionar.

   Observação: para detectar os nós automaticamente e adicioná-los à lista Nome do nó, consulte o tópico Configurar programações de detecção para obter mais detalhes.
6. Na lista Nós detectados, clique nos nós que deseja adicionar e clique na seta à direita. Os nós são adicionados à lista Nós para proteger.

7. Clique em Avançar para abrir a tela Credenciais do nó.
8. Forneça um nome de usuário e senha para cada nó que deseja adicionar ou especificar as credenciais global apropriadas.

   Clique em Concluir.

   Os nós selecionados são adicionados à lista Nomes dos nós, na tela Nó para o grupo de nós selecionado.
9. (Opcional) Clique em Atualizar. O servidor adicionado é relacionado agora na lista Grupos, na tela Nó.
10. (Opcional) Clique em Detectar e repita as etapas anteriores até que todos os servidores sejam adicionados.

Adicionar nós

À medida que o ambiente cresce, é possível usar a tela Nó para adicionar nós e atribui-los a grupos que deseja gerenciar dentro do aplicativo. O aplicativo adiciona somente máquinas virtuais onde:

- O sistema operacional convidado é Windows
- A versão do hardware VMware é 7 ou mais recente.

Você pode adicionar nós usando os seguintes processos:

- Adicionar nós a partir do resultado da detecção (na página 45) - a detecção permite fornecer detalhes do ESX e vCenter Server, detectar máquinas virtuais em execução em cada servidor e, em seguida, adicionar manual ou automaticamente nós detectados ao aplicativo, onde podem ser gerenciados e protegidos.

  Os servidores adicionados à lista Detectar são verificados de acordo com a programação especificada na tela Configuração até que sejam removidos. Não será necessário fornecer os detalhes do servidor novamente. A lista Detectar exibe apenas máquinas virtuais novas adicionadas a um servidor desde a última verificação. Ela não mostra as VMs já gerenciadas no aplicativo. É possível também executar a detecção sem precisar esperar a próxima verificação programada.
- Importar máquinas virtuais do vCenter/ESX (na página 46)

  Esta opção é um processo manual. O processo exige que você especifique os detalhes do ESX ou vCenter Server cada vez que iniciá-lo. É possível adicionar servidores à lista de detecção se quiser evitar fornecer os detalhes do servidor novamente. Esta opção lista todas as máquinas virtuais detectadas no servidor especificado, mesmo se já forem gerenciadas no aplicativo.

Adicionar nós a partir do resultado da detecção

Esta opção permite selecionar os nós que são detectados automaticamente com base nas configurações especificadas no painel Configuração da detecção.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Clique em Nós na barra de navegação para abrir a tela Nós.

2. Na categoria Nó, clique em Adicionar e, em seguida, clique em Adicionar nós a partir do resultado da detecção no menu pop-up.

   A tela Adicionar nós a partir do resultado da detecção é exibida, mostrando uma lista dos nós detectados.

3. Na lista Nós detectados, selecione os nós que deseja adicionar e clique na seta para adicioná-los à lista Nós para proteger. Clique em Avançar ao terminar.

   Observação: é possível filtrar a lista por nome do nó ou domínio para reduzir a lista.

4. (Opcional) Selecione um ou mais nós e clique em Ocultar nós selecionados para ocultar nós que não deseja fazer backup.

5. (Opcional) Verifique a opção Mostrar nós ocultos para exibir nós ocultos novamente na lista Nós detectados. Para ocultar os nós novamente, desmarque a opção.

6. Na tela Credenciais do nó, forneça um nome de usuário e uma senha para o nó que deseja adicionar. É possível especificar credenciais globais ou aplicar credenciais aos nós selecionados.

7. Clique em Concluir.

Os nós são adicionados.

Importar máquinas virtuais do vCenter/ESX

Também é possível adicionar nós usando a opção Importar máquinas virtuais do vCenter/ESX Server. Essa tarefa permite que o aplicativo detecte todas as máquinas virtuais em execução no host especificado, mas não executa verificações periódicas automáticas. Se as máquinas virtuais forem adicionadas posteriormente, repita esse procedimento ou as novas máquinas virtuais não serão reconhecidas.

Considere as seguintes diferenças entre esta opção e a tarefa Detectar:

- Especifique os detalhes do ESX e vCenter Server toda vez que iniciar esta opção.
- Você tem a opção de adicionar quaisquer servidores especificados à lista Detecção para que não precise digitar sempre as credenciais.
- Todas as máquinas virtuais disponíveis são listadas a cada vez que você usar esta opção. Até mesmo as máquinas virtuais gerenciadas pelo aplicativo são listadas.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Clique em Nó na barra de navegação para abrir a tela Nó.

2. Na barra de ferramentas, clique em Adicionar e em Importar máquinas virtuais do vCenter/ESX no menu pop-up.

   A caixa de diálogo Detectar nós é aberta.

3. Preencha os campos a seguir da caixa de diálogo Detectar nós:

   - Host do vCenter/ESX

     Observação: como melhor prática, especifique o nome do host ou endereço IP do sistema vCenter Server ao importar máquinas virtuais quando estiver executando o DRS (VMware Distributed Resource Scheduling) em seu ambiente. Essa abordagem ajuda a garantir que o CA ARCserve Central Host-Based VM Backup detecte máquinas virtuais em execução em seu ambiente, bem como backups do DRS em máquinas virtuais ativas que foram concluídos com êxito. Para evitar a falha de backup quando máquinas virtuais se movem entre os servidores ESX, é recomendável que você não especifique o nome do host ou endereço IP do servidor ESX ao importar máquinas virtuais.

     Para obter mais informações sobre o Distributed Resource Scheduling, consulte o site da VMware.

   - Nome de usuário
   - Senha
   - Porta
   - Protocolo

   Clique em Conectar e aguarde até que a verificação esteja concluída.

4. (Opcional) Ative a opção Adicionar automaticamente o servidor ESX/vCenter à lista da detecção.
5. Clique em Avançar para abrir a caixa de diálogo Credenciais do nó.
6. Na tela Credenciais do nó, forneça um Nome de usuário global e Senha para todas as máquinas virtuais detectadas e clique em Aplicar aos itens selecionados. Ou clique em uma VM para inserir credenciais específicas.
7. Clique em Concluir.

As máquinas virtuais selecionadas são adicionadas ao grupo de nós especificado.

Observação: o CA ARCserve Central Host-Based VM Backup não pode detectar os nomes de máquinas virtuais que estejam desligadas ou se o VMware Tools não estiver instalado. Sob essas condições, o campo Nome do host na tela Nó aparece como Desconhecido depois que os nós são importados. Além disso, o filtro Nome de nó (na tela Nó) não pode filtrar nós nomeados como Desconhecido.

Atualizar nós

O CA ARCserve Central Host-Based VM Backup permite atualizar informações sobre nós adicionados anteriormente.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, selecione Nó.

   A tela Nó é exibida.

2. Na barra Grupos, clique no grupo Todos os nós ou clique no nome de grupo contendo os nós que deseja atualizar.

   Os nós associados ao grupo são exibidos na lista de nós.

3. Clique nos nós que deseja atualizar e, em seguida, clique em Atualizar nó no menu pop-up.

   A caixa de diálogo Atualizar nó é exibida.

   Observação: para atualizar todos os nós no grupo de nós, clique com o botão direito do mouse no nome do grupo de nós e, em seguida, clique em Atualizar nó no menu pop-up.

4. Atualize os detalhes do nó, conforme necessário.

   Observação: para atualizar vários nós na lista de nós, selecione os nós desejados, clique com o botão direito do mouse em qualquer nó e clique em Atualizar nó no menu pop-up. O nome de usuário e a senha são os mesmo para todos os nós selecionados. Por padrão, a opção e o Especificar novas credenciais e a caixa de seleção Assumir controle do nó estão selecionados. É possível especificar um novo nome de usuário e senha para os nós selecionados e é possível forçar este servidor a administrar os nós. Além disso, é possível selecionar Usar credenciais existentes para aplicar o nome de usuário e senha atuais. Os campos são desativados.

5. Clique em OK.

   A caixa de diálogo Atualizar nó é fechada e os nós são atualizados.

Atualizar nós e diretivas depois de alterar o nome do host no servidor do CA ARCserve Central Applications

Depois de alterar o nome do host do servidor do CA ARCserve Central Host-Based VM Backup, atualize os nós e as diretivas aplicadas aos nós. Realize essas tarefas para manter a relação entre o servidor e os nós que o servidor está protegendo. A tabela abaixo descreve os possíveis cenários e a ação corretiva para cada cenário.

Cenário	Ação corretiva
O nó foi adicionado depois que o nome do host do servidor do CA ARCserve Central Host-Based VM Backup foi alterado.	Nenhuma ação corretiva é necessária.
O nó foi adicionado antes do nome de host do servidor do CA ARCserve Central Host-Based VM Backup ter sido alterado e a diretiva não foi aplicada ao nó.	Atualize o nó. Para obter mais informações, consulte Atualizar nós (na página 47).
O nó foi adicionado antes do nome de host do servidor do CA ARCserve Central Host-Based VM Backup ser alterado e da diretiva ser aplicada ao nó.	Aplique a diretiva novamente. Para obter mais informações, consulte Atribuir diretivas a máquinas virtuais.

Excluir nós

É possível excluir nós, conforme necessário.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Clique em Nó na barra de navegação para abrir a tela Nó.

2. Na barra de Grupos, clique no grupo Todos os nós ou clique no nome de grupo contendo o nó que você deseja excluir.

   Os nós associados ao grupo são exibidos na lista de nós.

3. Selecione um ou mais nós que desejar excluir e, em seguida, clique em Excluir na barra de ferramentas.

   Uma mensagem de confirmação é exibida.

4. Siga um destes procedimentos:

   - Clique em Sim para excluir o nó.
   - Clique em Não se não desejar excluir o nó.

Opções da tarefa de mesclagem

O CA ARCserve Central Host-Based VM Backup permite pausar e retomar tarefas de mesclagem para cada nó, a qualquer momento. O processo de pausa e retomada de tarefas de mesclagem não afeta as tarefas em andamento.

Pausar uma tarefa de mesclagem em um nó

O CA ARCserve Central Host-Based VM Backup permite pausar uma tarefa de mesclagem em um nó específico.

Por exemplo, as tarefas de mesclagem podem consumir recursos do sistema e fazer com que tarefas de backup sejam executadas com lentidão. Use a opção de pausa para interromper uma tarefa de mesclagem em andamento de modo que as tarefas de backup em andamento possam ser concluídas com a maior eficiência possível. Após a conclusão dos backups, é, então, possível retomar a tarefa de mesclagem.

Siga estas etapas:

1. Na página inicial do CA ARCserve Central Host-Based VM Backup, clique em Nó na barra Navegação para abrir a tela Nó.
2. Selecione o grupo de nós que contém os nós com tarefas de mesclagem a serem pausadas.

   Uma lista de nós para o grupo de nós selecionado é exibida.

3. Clique nos nós com as tarefas de mesclagem a serem pausadas. Em seguida, clique com o botão direito do mouse nos nós selecionados e clique em Pausar tarefa de mesclagem no menu pop-up.

   Observação: por padrão, a opção Pausar tarefa de mesclagem está desativada. Quando o nó está executando uma tarefa de mesclagem, conforme indicado na coluna de tarefas, a opção Pausar tarefa de mesclagem é ativada.

A tarefa de mesclagem do nó selecionado é pausada e pode ser verificada na página inicial do CA ARCserve D2D.

Retomar uma tarefa de mesclagem em um nó

O CA ARCserve Central Host-Based VM Backup permite retomar tarefas de mesclagem que foram pausadas para um nó específico.

Siga estas etapas:

1. Na página inicial do CA ARCserve Central Host-Based VM Backup, clique em Nó na barra Navegação para abrir a tela Nó.
2. Selecione o grupo de nós que contém os nós com tarefas de mesclagem a serem retomadas.

   Uma lista de nós para o grupo de nós selecionado é exibida.
3. Clique nos nós com tarefas de mesclagem pausadas que você agora deseja retomar. Em seguida, clique com o botão direito do mouse nos nós selecionados e clique em Retomar tarefa de mesclagem no menu pop-up.

   Observação: a opção Retomar tarefa de mesclagem é ativada quando uma tarefa de backup não está em execução, e as tarefas de mesclagem estão pausadas.

A tarefa de mesclagem do nó selecionado é retomada e pode ser verificada na página inicial do CA ARCserve D2D.

Como gerenciar tarefas de grupos de nós do CA ARCserve Central Host-Based VM Backup

Com o CA ARCserve Central Host-Based VM Backup, um Gerente de Armazenamento pode proteger várias máquinas virtuais tão facilmente quanto protegeria apenas uma.

Comece adicionando nós. É possível agrupar nós por aplicativo ou por sua finalidade. Criar um grupo de nós permite visualizar facilmente o ambiente de máquina virtual. Você pode criar diretivas de backup e atribuir uma diretiva a nós para simplificar a proteção de seu ambiente virtual. Para obter mais detalhes, consulte o tópico Como gerenciar diretivas do CA ARCserve Central Host-Based VM Backup (na página 72).

A ilustração a seguir descreve as tarefas que você pode executar para grupos de nós:

Este cenário descreve os seguintes tópicos:

- Adicionar grupos de nós (na página 52)
- Excluir grupos de nós (na página 54)
- Modificar grupos de nós (na página 55)

Adicionar grupos de nós

Ao importar inicialmente uma máquina virtual de um host ESX ou vCenter Server, um novo grupo de nós é automaticamente adicionado.

Os grupos de nós permitem gerenciar um grupo de computadores de origem do CA ARCserve D2D de acordo com características comuns. Por exemplo, é possível definir grupos de nós classificados pelo departamento que eles suportam: contabilidade, marketing, jurídico, recursos humanos e assim por diante.

O aplicativo contém os seguintes grupos de nós:

- **Grupos padrão:**
  - **Todos os nós -** contém todos os nós associados ao aplicativo.
  - **Nós sem um grupo** - contém todos os nós associados ao aplicativo que não estão atribuídos a um grupo de nós.
  - **Nós sem uma diretiva** - contém todos os nós associados ao aplicativo que não possuem uma diretiva atribuída.
  - **Servidor SQL -** contém todos os nós associados ao aplicativo e o Microsoft SQL Server está instalado no nó.
  - **Exchange -** contém todos os nós associados ao aplicativo e o Microsoft Exchange Server está instalado no nó.

  Observação: não é possível modificar ou excluir os grupos de nós padrão.
- **Grupos personalizados--**contém grupos de nós personalizados.
- **Grupos de vCenter/ESX**-- ao adicionar um nó a partir da opção Importar máquinas virtuais do vCenter/ESX, o nome do servidor de ESX/vCenter será adicionado a este grupo.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, clique em Nó para abrir a tela Nó.
2. Clique em Adicionar na barra de ferramentas Grupo de nós.

   A caixa de diálogo Adicionar grupo é aberta e nós aparecem na lista de Nós disponíveis.
3. Especifique um nome de grupo para o grupo de nós.

4. Preencha os campos abaixo na caixa de diálogo Adicionar grupo:
   - **Grupo--**selecione o nome do grupo que contém os nós que deseja atribuir.
   - **Filtro Nome do nó--**permite filtrar os nós disponíveis com base em critérios comuns.

     Observação: o filtro Nome do nó suporta o uso de caracteres curinga.

     Por exemplo, usar o Acc* permite filtrar todos os nós com um nome de nó que comece com Acc. Para limpar os resultados do filtro, clique em X no campo Filtro.
5. Para adicionar nós ao grupo de nós, selecione um ou mais nós que deseja adicionar e clique na seta à direita.

   Os nós passam da lista Nós disponíveis para a lista Nós selecionados e são atribuídos ao grupo de nós.

   Observação: para selecionar e mover todos os nós do grupo atual, clique na seta dupla à direita.
6. (Opcional): para mover todos os nós da lista Nós selecionados para a lista Nós disponíveis, clique na seta simples à esquerda.

   Observação: para selecionar e mover todos os nós do grupo atual, clique na seta dupla à esquerda.
7. Clique em OK.

O Grupo de nós é adicionado.

Excluir grupos de nós

É possível excluir um grupo de nós, conforme a necessidade. Quando um grupo que foi adicionado manualmente é excluído, as máquinas virtuais não são removidas do aplicativo. No entanto, se você excluir um grupo que foi criado automaticamente por uma detecção ESX ou vCenter Server, o grupo e todas as máquinas virtuais serão excluídos do aplicativo.

O aplicativo permite excluir os Grupos de nós que você criou.

Não é possível excluir os seguintes grupos de nós:

- **Todos os nós -** contém todos os nós associados ao aplicativo.
- **Nós sem um grupo** - contém todos os nós associados ao aplicativo que não estão atribuídos a um grupo de nós.
- **Nós sem uma diretiva** - contém todos os nós associados ao aplicativo que não possuem uma diretiva atribuída.
- **SQL Server -** contém todos os nós associados ao aplicativo, e o Microsoft SQL Server está instalado nos nós.
- **Exchange -** contém todos os nós associados ao aplicativo, e o Microsoft Exchange Server está instalado nos nós.

Observação: o processo de exclusão dos grupos de nós não exclui nós individuais do aplicativo.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, clique em Nó para abrir a tela Nó.

2. Clique no grupo de nós que você deseja excluir e, em seguida, clique em Excluir na barra de ferramentas do grupo de nós.

   A caixa de diálogo de Mensagem de confirmação é aberta.

3. Se tiver certeza de que deseja excluir o grupo de nós, clique em Sim.

   Observação: clique em Não se você não deseja excluir o grupo de nós.

O grupo de nós é excluído.

Modificar grupos de nós

O aplicativo permite modificar os grupos de nós que você criou. Você pode adicionar e remover nós de grupos de nós e alterar o nome de grupos de nós.

Observação: não é possível modificar as seguintes grupos de nós:

- **Todos os nós -** contém todos os nós associados ao aplicativo.
- **Nós sem um grupo** - contém todos os nós associados ao aplicativo que não estão atribuídos a um grupo de nós.
- **Nós sem uma diretiva** - contém todos os nós associados ao aplicativo que não possuem uma diretiva atribuída.
- **SQL Server -** contém todos os nós associados ao aplicativo e o Microsoft SQL Server está instalado.
- **Exchange -** contém todos os nós associados ao aplicativo e o Microsoft Exchange Server está instalado.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na Barra de navegação na página inicial, clique em Nó.

   A tela Nó é exibida.

2. Clique no grupo de nós que deseja modificar e, em seguida, clique em Modificar na barra de ferramentas Grupo de nós.

   A caixa de diálogo Modificar grupo é aberta.

3. Para modificar o Nome do grupo, especifique um novo nome no campo Nome do grupo.

4. Para adicionar nós ao grupo de nós, selecione um ou mais nós para adicionar ao grupo de nós e clique na seta à direita.

   Os nós passam da lista Nós disponíveis para a lista Nós selecionados e são atribuídos ao grupo de nós.

   Observação: para mover todos os nós da lista Nós disponíveis para a lista Nós selecionados, clique na seta dupla à direita.

5. Para remover nós do grupo de nós, clique na seta à esquerda ou na seta dupla à esquerda para remover um dos nós ou todos eles, respectivamente.

6. (Opcional) Para filtrar os nós disponíveis com base em critérios comuns, especifique um valor de filtragem no campo Filtragem pelo nome do nó.

   Observação: o campo Filtro permite o uso de caracteres curinga.

   Por exemplo, usar o Acc* permite filtrar todos os nós com um nome de nó que comece com Acc. Para limpar os resultados do filtro, clique no X no campo Filtro.

7. Clique em OK.

O grupo de nós é modificado.

Atualizar detalhes do ESX e vCenter Server

O CA ARCserve Central Host-Based VM Backup permite atualizar detalhes do vCenter e ESX Server que foram adicionados anteriormente.

Siga estas etapas:

1. Na tela Nó, expanda Grupos do vCenter/ESX da barra Grupos.
2. Selecione o grupo vCenter/ESX do qual deseja atualizar os detalhes do servidor e, em seguida, clique com o botão direito do mouse e clique em Atualizar vCenter/ESX.

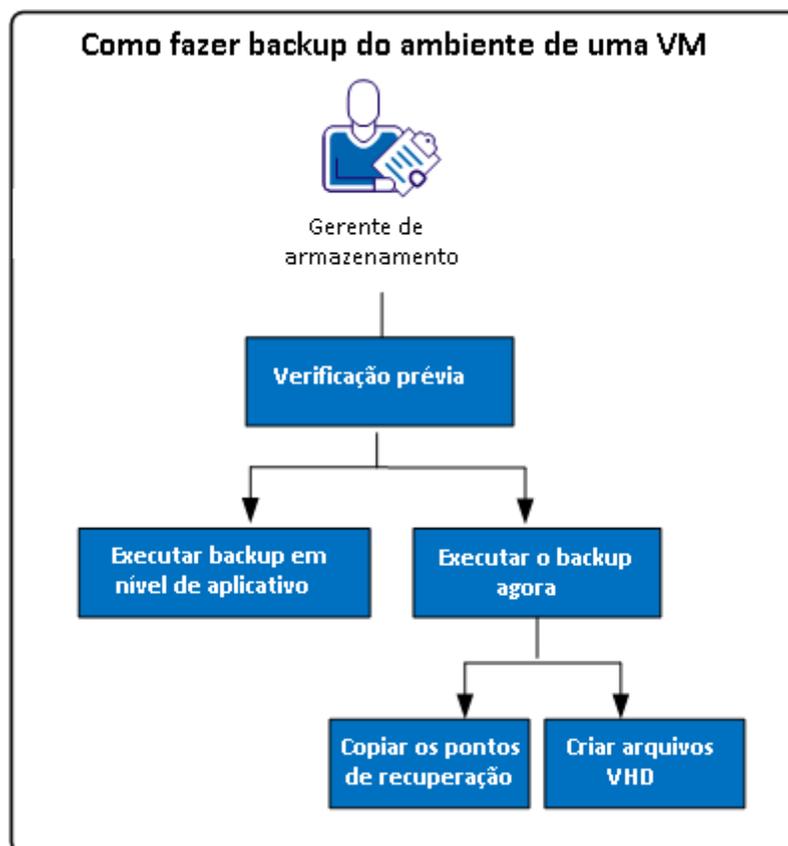
   A caixa de diálogo Atualizar vCenter/ESX é exibida.

3. Atualize os detalhes do vCenter/ESX Server de maneira adequada.
4. Clique em OK.

   A caixa de diálogo Atualizar vCenter/ESX é fechada e o grupo de nós é atualizado.

Como fazer backup do ambiente de máquina virtual

Este cenário explica como um Gerenciador de Armazenamento pode fazer backup e proteger todas as máquinas virtuais no seu ambiente.

O diagrama a seguir ilustra como fazer backup do ambiente de máquina virtual.

A lista a seguir descreve os processos que estão ilustrados no diagrama:

- Executar verificações prévias para as tarefas de backup (na página 58)
- Executar um backup agora (na página 62)
  - Copiar os pontos de recuperação de backup (na página 64)
  - Criar arquivos VHD (na página 68)
- Executar backups em nível de aplicativo (na página 68)

Executar verificações prévias para as tarefas de backup

O CA ARCserve Central Host-Based VM Backup oferece um utilitário chamado de PFC (Preflight Check - Verificação Prévia), que permite fazer verificações vitais em nós específicos para detectar condições que podem ocasionar a falha das tarefas de backup. A PFC é executada automaticamente quando você executa as seguintes ações:

- Importar máquinas virtuais de um sistema vCenter/ESX Server
- Adicionar nós a partir do resultado da detecção
- Atualizar um nó

Além disso, também é possível executar uma verificação prévia manualmente.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Clique em Nós na barra de navegação para abrir a tela Nós.

2. Execute uma das seguintes ações para especificar os nós em que deseja executar a verificação prévia em:

   - **Nível de nó**: clique no grupo que contém os nós em que deseja executar a verificação prévia e, em seguida, clique na caixa de seleção ao lado dos nós. Em seguida, clique com o botão direito do mouse nos nós e clique em Verificação prévia no menu de contexto.
   - **Nível de grupo**: clique com o botão direito do mouse no grupo que contém os nós e clique em Verificação prévia.

   A mensagem Iniciando a verificação prévia da máquina virtual é exibida.

3. Role para a coluna Status de PFC e exiba o status da verificação prévia.

A tabela a seguir descreve as verificações executadas pela PFC:

Item	Descrição
CBT	(CBT) é um recurso que rastreia os setores do disco localizados em uma máquina virtual que foi alterada. Isso ajuda a reduzir o tamanho dos backups. Este item verifica se o CBT está ativado.
VMware Tools	Este item verifica se as ferramentas de VMware estão instaladas em cada máquina virtual.
Discos	Este item verifica os discos da máquina virtual.
Estado da energia	Este item verifica se a máquina virtual está ligada.
Credenciais	Este item verifica se as credenciais do usuário são válidas.

Item	Descrição
Aplicativos	Este item verifica se o Microsoft SQL Server e o Microsoft Exchange Server está instalado ou não.

Para obter mais informações sobre a resolução de erros e avisos dos resultados da verificação prévia, consulte o tópico Soluções para itens de verificação prévia (na página 59).

Soluções para itens de verificação prévia

As tabelas a seguir descrevem as soluções para ajudá-lo a resolver erros e avisos dos resultados da verificação prévia:

CBT

Status	Mensagem	Solução
Aviso	O Rastreamento de Bloco Alterado é ativado com os instantâneos presentes. Um backup completo do disco será aplicado.	Para aplicar o backup de bloco usado, execute as seguintes etapas: 1. Excluir todos os instantâneos associados à máquina virtual. 2. Efetuar logon no servidor do proxy do Host-Based VM. 3. Abra o editor de registro e procure a seguinte chave: HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFBackupDll\<VM-InstanceUUID> **Observação**: substitua <VM-InstanceUUID> pelo valor UUID da máquina virtual em que o CBT estiver falhando. O valor pode ser encontrado no URL da máquina virtual usada quando conectada ao CA ARCserve D2D. 4. Definir a chave de registro para "full disk backupForFullBackup"=0. 5. Criar/definir o registro para ResetCBT=1. 6. Envie a tarefa de backup.

VMware Tools

Status	Mensagem	Solução
Aviso	Desatualizado.	Instale a versão mais recente do VMware Tools.

Status	Mensagem	Solução
Aviso	Não instalado ou não está em execução.	Instale a versão mais recente do VMware Tools e certifique-se de que a ferramenta está em execução.

Discos

Status	Mensagem	Solução
Erro	Instantâneos de VM não são suportados para a VM, pois ela tem um controlador SCSI configurado para configuração de compartilhamento de barramento.	Use o CA ARCserve Central Protection Manager ou o CA ARCserve D2D para fazer backup da VM.
Aviso	Não será feito backup do disco físico de RDM (Raw Device Mapping - Mapeamento de Dispositivo Simples).	Use o CA ARCserve Central Protection Manager ou o CA ARCserve D2D para fazer backup da VM.
Aviso	O disco virtual de RDM será armazenado em backup como um disco cheio.	Use o CA ARCserve Central Protection Manager ou o CA ARCserve D2D para fazer backup da VM.
Aviso	Não será feito backup do disco independente.	Use o CA ARCserve Central Protection Manager ou o CA ARCserve D2D para fazer backup da VM.
Aviso	O aplicativo fará o backup do disco no repositório de dados do NFS (Network File System - Sistema de Arquivos de Rede) como um disco cheio.	Use o CA ARCserve Central Protection Manager ou o CA ARCserve D2D para fazer backup da VM.

Estado da energia

Status	Mensagem	Solução
Aviso	Desligado	Ligue a máquina virtual.
Aviso	Suspenso	Ligue a máquina virtual.

Credenciais

Status	Mensagem	Solução
Aviso	Credenciais incorretas.	Forneça credenciais do usuário válidas.
Aviso	Não fornecido.	Forneça credenciais do usuário válidas.

Aplicativos

Status	Mensagem	Solução
Aviso	A restauração em nível de aplicativo não é suportada porque a VM tem discos IDE.	Use o CA ARCserve Central Protection Manager ou o CA ARCserve D2D para fazer backup dos dados do Microsoft SQL Server e do Exchange Server.
Aviso	O VMware VIX não está instalado no servidor do host.	Baixe o VIX no site da VMware e instale-o no servidor host do CA ARCserve Central Applications.
Aviso	O VMware VIX no servidor do CA ARCserve Central Host-Based VM Backup está desatualizado.	Baixe o VIX no site da VMware e instale-o no servidor host do CA ARCserve Central Applications.
Aviso	A restauração em nível de aplicativo não é suportada porque não há suporte para o ESX Server.	Atualize o ESX Server para 4.1 ou superior, ou use o CA ARCserve Central Protection Manager ou o CA ARCserve D2D para fazer backup dos dados do Microsoft SQL Server e do Exchange Server.
Aviso	A restauração em nível de aplicativo não é suportada porque não há slots de SCSI suficientes disponíveis.	Use o CA ARCserve Central Protection Manager ou o CA ARCserve D2D para fazer backup dos dados do Microsoft SQL Server e do Exchange Server.
Aviso	A origem reside em um disco dinâmico. A restauração em nível de aplicativo não é suportada.	Use o CA ARCserve Central Protection Manager ou o CA ARCserve D2D para fazer backup dos dados do Microsoft SQL Server e do Exchange Server. **Observação**: o VMware não oferece suporte ao nível de aplicativo fechado em máquinas virtuais que estão no Windows Server 2008 ou posterior com discos dinâmicos em execução no ESX Server 4.1 ou posterior.
Aviso	Não foi possível recuperar informações sobre o aplicativo. Isso pode impedir que backups em nível de aplicativo sejam concluídos com êxito.	Forneça credenciais internas ou do administrador de domínio para efetuar logon no sistema operacional convidado da máquina virtual. Devido a uma limitação do VMware, o backup é compatível apenas com as VMs em execução em um ESX Server que possuem uma licença paga. Um backup não é suportado em servidores ESXi com uma licença gratuita.
Aviso	A recuperação no nível do aplicativo não é suportada em sistemas com espaços de armazenamento ativados. Somente a máquina virtual inteira pode ser recuperada.	Use o CA ARCserve Central Protection Manager ou o CA ARCserve D2D para fazer backup dos dados do Microsoft SQL Server e do Microsoft Exchange Server.

Executar um backup agora

Em geral, os backups são executados automaticamente e controlados pelas configurações da programação. No entanto, pode ser necessário executar um backup ad-hoc (completo, incremental ou de verificação) imediatamente.

Um backup ad hoc é realizado conforme necessário, em vez de agendado antecipadamente como parte de um plano de backup. Por exemplo, se você repetir a programação para backups completos, incrementais e de verificação e desejar fazer grandes alterações em seu computador, é possível executar um backup ad hoc imediato sem esperar até que o próximo backup programado ocorra.

Um backup ad hoc permite também adicionar um ponto de recuperação personalizado (não programado) para que seja possível reverter a este ponto anterior no tempo, se necessário. Por exemplo, se um patch ou service pack for instalado e, em seguida, for detectado que ele afeta negativamente o desempenho do computador, talvez você queira reverter para a sessão de backup ad hoc que não inclua o patch ou service pack.

Siga estas etapas:

1. Efetue logon no aplicativo.
2. Na barra de navegação na página inicial, clique em Nó para abrir a tela Nó.
3. Execute uma das seguintes ações para especificar os nós para backup:
   - **Nível de nó:** clique no grupo que contém os nós para backup e, em seguida, clique na caixa de seleção ao lado dos nós para backup.
   - **Nível de grupo:** clique no grupo que contém os nós para backup.
4. Em seguida, execute uma das seguintes ações para fazer backup do nó:
   - Na barra de ferramentas, clique em Backup.
   - Clique com o botão direito do mouse no grupo selecionado ou clique com o botão direito do mouse nos nós e, em seguida, clique em Fazer backup agora no menu de contexto.

5. Na caixa de diálogo Executar um backup agora, especifique o tipo de backup, clicando em um dos seguintes tipos:

   - **Backup completo--**inicia um backup completo de todo o computador ou de volumes selecionados.
   - **Backup incremental--**inicia um backup incremental do computador. Um backup incremental realiza backup somente dos blocos que foram alterados desde o backup anterior.

     Observação: as vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a execução de backups.
   - **Backup de verificação--**inicia um backup de verificação do computador, examinando o backup mais recente de cada bloco e comparando o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup para algum bloco não corresponder à origem, o CA ARCserve D2D atualizará (nova sincronização) o backup do bloco de dados que não corresponder. Considere as seguintes vantagens e desvantagens para executar backups de verificação:
     - Vantagens - uma imagem de backup muito pequena é produzida quando comparada ao backup completo porque somente os blocos alterados (blocos que não correspondam ao último backup) são armazenados em backup.
     - Desvantagens - o backup é mais demorado porque todos os blocos do disco de origem são comparados aos blocos do último backup.

   Observação: se você adicionar um novo volume à origem do backup, será feito um backup completo do volume recém-adicionado, independentemente do método de backup geral selecionado.

6. (Opcional) Especifique o Nome do backup e clique em OK. Se você não especificar um nome, ele será nomeado por padrão como Backup personalizado/completo/incremental/de verificação.

Uma tela de confirmação é exibida, e o tipo de backup selecionado é iniciado imediatamente.

Esteja ciente do seguinte:

- Todos os valores especificados nas caixas de diálogo Diretiva são aplicados à tarefa.
- Se houver falha em uma tarefa de backup personalizada (ad hoc), nenhuma tarefa de constituição será criada. Uma tarefa de constituição pode ser criada apenas para tarefas programadas com falha.
- O CA ARCserve Central Host-Based VM Backup aplica as seguintes tarefas de backup em ordem de prioridade:
  - Completo
  - Verificar
  - Incremental

  As condições a seguir ocorrem quando um Backup Agora é enviado e uma tarefa está aguardando na fila:

  - Quando uma tarefa de Backup Completo é enviada e uma tarefa de Backup de Verificação está na fila, a tarefa de Backup Completo substitui a tarefa na fila.
  - Quando uma tarefa de Backup Completo é enviada e uma tarefa de Backup Incremental está na fila, a tarefa de Backup Completo substitui a tarefa na fila.
  - Quando uma tarefa de Backup de Verificação é enviada e uma tarefa de Backup Incremental está na fila, a tarefa de Backup de Verificação substitui a tarefa na fila.
  - Quando uma tarefa de Backup de Verificação é enviada e uma tarefa de Backup Completo está na fila, a tarefa de Backup de Verificação será ignorada.
  - Quando uma tarefa de Backup Incremental é enviada e uma tarefa de Backup Completo está na fila, a tarefa de Backup Incremental é ignorada.
  - Quando uma tarefa de Backup Incremental é enviada e uma tarefa de Backup de Verificação está na fila, a tarefa de Backup Incremental é ignorada.

Copiar pontos de recuperação

Cada vez que o CA ARCserve D2D executa um backup com êxito, também é criada uma imagem de instantâneo pontual de seu backup. Este conjunto de pontos de recuperação permite localizar e especificar uma imagem de backup a ser copiada. Você pode fazer o seguinte para proteger seus backups:

- Copiar/exportar informações de ponto de recuperação para armazená-las com segurança fora do local, quando ocorrer uma catástrofe.
- Salvar seus pontos de recuperação em vários locais.
- Consolidar os backups se o destino estiver ficando cheio e você ainda desejar preservar todos os pontos de recuperação.

Ao selecionar um ponto de recuperação para copiar, você também captura todos os blocos de backups anteriores que são necessários para recriar uma imagem de backup completa e mais recente.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Clique em Nó na barra de navegação para abrir a tela Nó.

2. Na lista Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D com os pontos de recuperação que deseja copiar.

   A lista de nós exibe todos os nós associados ao grupo especificado.

3. Procure e clique no nó que deseja efetuar logon e, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   O CA ARCserve D2D abre e você é conectado à página inicial do nó do CA ARCserve D2D.

   Observação: garante que as opções de pop-up na janela do navegador estão ativadas.

4. Na página inicial do CA ARCserve D2D, selecione Copiar ponto de recuperação.

   A caixa de diálogo Copiar ponto de recuperação é exibida.

5. No campo Local do backup, especifique a origem do backup. Você pode especificar um local ou procurar o local onde as suas imagens de backup estão armazenadas. Clique no ícone de seta verde para verificar a conexão com o local especificado. Se necessário, forneça as credenciais de nome de usuário e senha para acessar esse local.

6. No campo Máquina virtual, clique na lista suspensa ao lado da opção Selecionar a máquina virtual para especificar a máquina virtual que contém os pontos de recuperação que deseja copiar.

   A visualização do calendário realça todas as datas do período exibido que contêm pontos de recuperação para essa origem de backup.

7. Especifique o ponto de recuperação a ser copiado.

   a. Selecione a data no calendário para a imagem de backup que deseja copiar.

      Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado e o nome do backup.

      Observação: um ícone de relógio com um símbolo de cadeado indica que o ponto de recuperação contém informações criptografadas e exige uma senha para a restauração.

   b. Selecione o ponto de recuperação que deseja copiar.

      O conteúdo do backup correspondente (incluindo aplicativos) para esse ponto de recuperação é exibido.

8. Clique em Avançar.

   A caixa de diálogo Opções de cópia é exibida.

Observação: dois campos de senha são exibidos nessa caixa de diálogo. O campo Senha é destinado à senha para descriptografar a sessão de origem e o campo Senha criptografada é usado para criptografar a sessão de destino.

a. Se o ponto de recuperação exportado tiver sido criptografado anteriormente, uma senha será necessária.

   - Se o ponto de recuperação exportado for uma sessão de backup da mesma máquina que está executando a tarefa de cópia de ponto de recuperação, a senha criptografada será salva e preenchida automaticamente.
   - Se o ponto de recuperação exportado for uma sessão de backup de outra máquina, uma senha criptografada será necessária.

b. Selecione o destino.

   Você pode especificar um local ou procurar o local onde a cópia do ponto de recuperação selecionado está armazenada. Clique no ícone de seta verde para verificar a conexão com o local especificado. Digite o nome de usuário e a senha, se necessário.

c. Selecione o nível de compactação a ser executado.

   Observação: o nível de compactação do backup especificado não tem relação com o nível de compactação da cópia. Por exemplo, no destino do backup, o nível de compactação pode ser definido como Padrão. No entanto, ao enviar a tarefa de cópia, a compactação pode ser alterada para Sem compactação ou Compactação máxima.

   A compactação é executada para reduzir o uso de espaço em disco, mas também tem um impacto inverso sobre a velocidade do backup devido ao aumento no uso da CPU.

   As opções disponíveis são:

   - **Sem compactação** - não será executada nenhuma compactação. Os arquivos estão no formato VHD puro. Essa opção exige menos uso da CPU (mais velocidade), mas também mais uso de espaço em disco para a imagem de backup.
   - **Compactação padrão** - alguma compactação será executada. Essa opção proporciona um bom equilíbrio entre o uso da CPU e o uso do espaço em disco. Essa opção é a configuração padrão.
   - **Compactação máxima** - a compactação máxima será executada. Essa opção proporciona maior uso da CPU (menos velocidade), mas também menos uso de espaço em disco para a imagem de backup.

   Considere os seguintes pontos:

   - Se a imagem de backup contiver dados não compactáveis (como imagens JPG, arquivos ZIP, etc.), espaço adicional de armazenamento será usado para lidar com esses dados. Como resultado, se você selecionar qualquer opção de compactação que possuir dados não compactáveis no backup, ele pode na verdade resultar em um aumento do uso de espaço em disco.
   - Caso altere o nível de compactação de Sem compactação para Compactação padrão ou Compactação máxima, ou ainda de Compactação padrão ou Compactação máxima para Sem compactação, o primeiro backup executado após esta alteração será automaticamente um Backup completo. Após a execução do backup completo, todos os backups futuros (completo, incremental ou de nova sincronização) serão executados conforme a programação.

d. Se deseja que o ponto de recuperação copiado também seja criptografado, forneça as seguintes informações:

   É possível alterar, adicionar ou remover a criptografia do ponto de recuperação copiado.

   - Selecione o tipo de algoritmo de criptografia usado para a cópia.

     As opções de formatação são Sem criptografia, AES-128, AES-192 e AES-256.
   - Fornecer (e confirmar) uma senha criptografada.

9. Clique em Criar uma cópia.

   Uma janela de notificação de status é exibida, e o processo de cópia do tipo de ponto de recuperação selecionado será iniciado imediatamente.

   Observação: o CA ARCserve D2D permite apenas que uma tarefa de cópia de ponto de recuperação seja executada ao mesmo tempo.

   A imagem do ponto de recuperação será copiada da origem do backup para o destino da cópia.

Criar arquivos VHD a partir do CA ARCserve Central Host-Based VM Backup

Este procedimento do CA ARCserve D2D permite criar um arquivo VHD (Virtual Hard Disk) do ponto de recuperação criado depois de cada backup bem-sucedido. Para obter mais informações, consulte o Apêndice do CA ARCserve D2D.

Siga estas etapas:

1. Execute o procedimento Copiar ponto de recuperação (na página 64).
2. Quando a cópia for concluída, navegue até o destino especificado e vá para o host do CA ARCserve D2D.
3. Abra a pasta VStore\S0000000001.
4. Localize todos os arquivos com uma extensão D2D e altere para VHD. Depois de renomear todos, é possível usá-los como arquivos VHD normalmente.

Executar backups em nível de aplicativo

Geralmente, nenhuma etapa especial é necessária para proteger os sistemas Microsoft Exchange ou SQL Server.

Para executar um backup completo de aplicativo, certifique-se de que os seguintes pontos são reconhecidos:

- Todos os gravadores do aplicativo se encontram em um estado estável. Use *vssadmin* para ver o status do gravador.
- Todos os bancos de dados cujo backup será feito se encontram em um estado íntegro. Por exemplo, para o SQL Server, certifique-se de que o status do banco de dados não seja *Restaurando*.

Também é possível truncar os logs de transação para o SQL e Exchange Servers separadamente.

Observação: se atualizar para um ESX Server, também deverá atualizar as ferramentas de VMware dentro dos sistemas operacionais convidados antes de executar backups em nível de aplicativo, para evitar erros de itens desatualizados.

Executar backups completos de disco que contenha apenas dados do bloco usado

A recuperação de dados do bloco usado após executar backups completos de disco ajuda a reduzir a janela de backup e o requisito de menos espaço a partir do destino do backup.

Observação: devido à limitação do VMware, os blocos usados não podem ser recuperados da máquina virtual quando existirem instantâneos do ponto de recuperação. Em tais casos, um backup completo do disco é executado na máquina virtual.

Depois que o backup completo do disco é enviado, execute as etapas a seguir para recuperar os dados do bloco usado:

1. Exclua todos os instantâneos associados à máquina virtual.
2. Efetue logon na máquina virtual do CA ARCserve Central Host-Based VM Backup.
3. Abra o editor de registro e procure a seguinte chave:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFBackupDll\VM_InstanceUUID
   ```

4. Defina a chave de registro full disk backupForFullBackup como 0.
5. Crie ou configure o registro ResetCBT como 1.
6. Envie a tarefa de backup.

Exibir informações de status da tarefa

O CA ARCserve Central Virtual Standby converte os pontos de recuperação do CA ARCserve D2D em instantâneos do ponto de recuperação. Você pode exibir informações de status sobre o andamento das tarefas do Host-Based VM Backup.

Quando uma tarefa estiver em execução, você poderá exibir informações detalhadas sobre ela. Também é possível interromper a tarefa atual.

Siga estas etapas:

1. Efetue logon no aplicativo.
2. Clique em Nós na barra de navegação para abrir a tela Nós.
3. Se houver tarefas do Host-Based VM Backup em andamento, a fase da tarefa será exibida no campo Tarefa, como ilustrado pela seguinte tela:

4. Clique na fase para abrir a caixa de diálogo Monitor de status de backup.

   Observação: para obter informações sobre os campos que aparecem no monitor de status de backup, consulte o tópico Monitor de status de backup (na página 70).

5. Execute uma das opções a seguir:

   - Clique em Fechar para fechar a caixa de diálogo Monitor de status de backup.
   - Clique em Cancelar para interromper a tarefa atual.

     Observação: a caixa de diálogo Monitor de status de backup será fechada imediatamente depois de clicar em Cancelar.

Mais informações:

Exibir informações de status da tarefa (na página 69)

Tarefas de monitoramento de backup da máquina virtual com base no host

É possível exibir o status dos backups de máquinas virtuais na tela Nó. Procure o nó que tem uma tarefa em andamento no campo Tarefa, clique no link e, em seguida, essa caixa de diálogo será aberta.

Os backups da máquina virtual são realizados em duas fases. Primeiro, os discos rígidos virtuais são armazenados em backup e, em seguida, se bem-sucedido, o catálogo é gerado. O catálogo permite restaurar arquivos e pastas, bem como a máquina virtual inteira.

O monitor exibe as seguintes informações em tempo real sobre a tarefa de status do backup:

- **Fase - (Monitores de status de backup e do catálogo)** exibe o ponto atual no processo representado pela parte sombreada da barra de progresso.
- **Hora de início - (Monitores de status de backup e do catálogo)** exibe a data e a hora em que a operação foi iniciada com base na configuração da diretiva.
- **Tempo decorrido - (Monitores de status de backup e do catálogo)** exibe a diferença entre a hora de início e a hora atual.
- **Tempo restante estimado - (somente o Monitor de status de backup)** exibe o tempo estimado para conclusão da tarefa.
- **Processando** - **(somente o Monitor de status do catálogo)** exibe a letra de unidade de volume ou o aplicativo para o qual o catálogo está sendo gerado no momento.

- **Espaço poupado com a compactação - (somente o Monitor de status de backup)** exibe a parte do espaço em disco poupado se a compactação foi especificada na diretiva da operação de backup.
- **Nível de compactação** - **(somente o Monitor de status de backup)** exibe o tipo de compactação usado para backups. As opções podem ser Sem compactação, Compactação padrão (padrão) ou Compactação máxima.
- **Criptografia - (somente o Monitor de status de backup)** exibe o método de criptografia selecionado quando a tarefa de backup foi configurada.
- **Limite de velocidade de gravação - (somente o Monitor de status de backup)** exibe o valor se o Acelerador de backup tiver sido definido na tela Configurações de proteção da diretiva de backup.
- **Velocidade de gravação - (somente o Monitor de status de backup)** exibe a velocidade real de gravação em megabytes por minuto.
- **Velocidade de leitura - (somente o Monitor de status de backup)** exibe a velocidade real de leitura em megabytes por minuto.

Como gerenciar diretivas do CA ARCserve Central Host-Based VM Backup

As diretivas de backup definem como e quando fazer backup de nós que são importados do vCenter/ESX Server. Os Gerenciadores de Armazenamento podem criar e editar diretivas de backup e atribuir e desatribuir dos nós.

Observação: é possível atribuir uma diretiva a um ou mais nós. No entanto, você não pode atribuir uma ou mais diretivas a um nó.

O diagrama a seguir ilustra o processo de administração de diretivas de backup.

A lista a seguir descreve os processos que estão ilustrados no diagrama:

- Criar diretivas de backup (na página 73)
- Editar diretivas de backup (na página 77)
- Atribuir e remover a atribuição de nós de diretivas de backup (na página 80)

Criar diretivas de backup

O processo de criação de diretivas de backup usa a interface do CA ARCserve D2D para definir configurações de backup, com algumas distinções. É possível criar diretivas com base em necessidades de backup semelhantes, por exemplo, por aplicativo instalado ou por programação.

O procedimento a seguir resume as etapas necessárias para criar uma diretiva de tarefa de backup simples do CA ARCserve D2D. Para obter detalhes completos sobre a criação de diretivas de backup do CA ARCserve D2D, consulte os tópicos no apêndice.

Observação: durante uma operação de backup com base no host, a seguinte mensagem será exibida se estiver usando o hotadd como modo de transporte:

É preciso formatar o disco na unidade <driveLetter> antes de usá-lo. Deseja formatá-lo?

Selecione Cancelar para ignorar esta mensagem. A mensagem ocorre quando o sistema operacional detecta que o disco rígido virtual foi adicionado ao servidor proxy de backup. O sistema operacional pressupõe que o disco rígido virtual é um novo dispositivo que exige formatação. Se clicar em Formatar disco incorreto, nenhum dano ocorrerá, pois o disco rígido virtual é somente leitura.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Clique em Diretivas na barra de navegação para abrir a tela Diretivas.

2. Clique em Novo na barra de ferramentas para abrir a caixa de diálogo Nova diretiva.

3. Digite um Nome da diretiva que descreve a diretiva adequadamente.

4. Na guia Configurações de backup, clique em Configurações de proteção e especifique as seguintes informações:

   - **Destino do backup** - especifique o volume local ou a pasta compartilhada remota na qual deseja salvar suas sessões de backup.
   - **Proxy de backup de VM do CA ARCserve D2D** - especifique o nome do host ou endereço IP do servidor em que o CA ARCserve D2D foi instalado. Se o CA ARCserve D2D ainda não estiver instalado, você poderá usar o CA ARCserve Central Protection Manager para implantá-lo. Forneça as credenciais apropriadas ao servidor. O número de porta padrão é 8014. Se tiver alterado esse padrão durante a instalação do CA ARCserve D2D, especifique o número de porta correto.
   - **Configuração de retenção** -- é possível definir a diretiva de retenção com base no número de pontos de recuperação a serem retidos (mescla sessões) ou com base no número de conjuntos de recuperação a serem retidos (exclui conjuntos de recuperação e desativa os itens incrementais ininterruptos). A opção padrão é Reter pontos de recuperação. Para obter mais detalhes, consulte Especificar configurações de proteção, no Guia do Usuário do CA ARCserve Central Protection Manager.
   - **Compactação** - selecione um nível de compactação. O valor padrão é Padrão. É possível especificar a opção Sem compactação ou Compactação máxima.
   - **Criptografia** - escolha um nível de criptografia. O valor padrão é Sem criptografia. Se escolher um nível de criptografia, você deverá fornecer uma senha criptografada, usada para restaurar dados criptografados.
   - **Acelerador de backup** - digite a taxa em que os backups são gravados em disco. Diminua essa taxa para reduzir a carga da CPU ou de rede, mas observe que isso aumenta a janela de backup. Esta opção é ativada, por padrão.

5. Clique em Programar e preencha as seguintes informações:

   - **Data e hora de início**-- especifique a data e a hora em que deseja iniciar as tarefas de backup.
   - **Backup incremental** - defina uma programação repetida para as tarefas de backup incremental. O valor padrão é repetir os backups incrementais uma vez por dia.
   - **Backup completo** - defina uma programação repetida para as tarefas de backup completo. Por padrão, o valor é definido para Nunca se repetir.
   - **Backup de verificação** - defina uma programação de repetição para as tarefas de backup de verificação. Por padrão, o valor é definido para Nunca se repetir.

6. Clique em Avançado e preencha as seguintes informações:

   - **Truncar log** - ative as seguintes opções se desejar truncar os arquivos de log do aplicativo:

     - **SQL Server** - escolha uma programação de truncamento diária, semanal ou mensal.

     - **Exchange Server** - escolha uma programação de truncamento diária, semanal ou mensal.

   - **Reservar espaço no destino** - especifique a porcentagem de espaço a ser reservado para a execução de um backup. Essa quantidade de espaço contínuo é, então, imediatamente reservada no destino antes que o backup comece a gravar os dados, e ajuda a acelerar o backup.

   - **Catálogos** - selecione a opção Gerar catálogo do sistema de arquivos para agilizar a pesquisa depois de cada backup para reduzir o tempo de espera de pesquisa do navegador.

     Se essa opção não estiver selecionada, as restaurações poderão ser executadas imediatamente após o backup sem precisar esperar até que a tarefa seja concluída. Por padrão, essa opção está desativada. Lembre-se das seguintes considerações:

     - Ao gerar um catálogo do sistema de arquivos para cada tarefa de backup, isso resulta em uma maior quantidade de armazenamento em disco necessária para armazenar os arquivos de metadados e os arquivos de catálogos e um aumento no uso da CPU. Além disso, se a origem do backup contiver vários arquivos, o processo de geração de um catálogo pode ser uma tarefa demorada.

     - Quando você seleciona volumes ReFS como a origem do backup, os catálogos não podem ser gerados. A mensagem de aviso é exibida, informando sobre esta condição.

7. Clique em Configurações de backup anterior ou posterior e especifique os comandos de backup anterior ou posterior desejados. Se necessário, forneça as credenciais corretas:
   - **Executar um comando antes do início do backup** - digite o comando de script a ser executado antes do início da tarefa de backup.
   - **No código de saída**-- ative essa opção para disparar o comando de script em um código de saída específico.
   - **Executar tarefa** - caso selecionada, o software continuará executando a tarefa se o código de saída especificado for retornado.
   - **Cancelar tarefa** - caso selecionada, o software anulará a tarefa se o código de saída especificado for retornado.
   - **Executar um comando depois de gerar um instantâneo** - digite o comando de script a ser executado depois que o instantâneo for gerado.
   - **Executar um comando quando o backup terminar** - digite o comando de script a ser executado depois que o backup for concluído.
8. (Opcional) Clique na guia Preferências. Configurar qualquer alerta de email a seguir, conforme necessário:
   - Tarefas não executadas
   - O vCenter/ESX não pode ser atingido (antes do backup)
   - Falha na licença
   - Backup, catálogo, restaurar ou copiar falha/paralisação/cancelamento da tarefa
   - Backup, catálogo, restaurar ou copiar a tarefa com êxito
   - O espaço livre do destino é menor que
   - A tarefa de mesclagem foi interrompida, ignorada, com falha ou paralisada
   - Tarefa de mesclagem com êxito
   - Ignorar/Mesclar tarefa em espera na fila de tarefas

Se ativar essas opções, clique em Configurações de email para configurar o servidor de email. Forneça o tipo de serviço, servidor de email e porta. Se a autenticação for necessária, ative a opção e forneça as credenciais.

- Especifique o assunto a ser exibido no email, por exemplo, Alerta do CA ARCserve Central Host-Based VM Backup.
- Especifique um valor De, por exemplo, CA ARCserve Central Host-Based VM Backup.
- Especifique um endereço de email para todos os destinatários. Separe cada endereço com um ponto e vírgula (;).

É possível ativar as configurações de proxy ao fornecer o nome do servidor proxy, a porta e as credenciais necessárias.

Clique em OK.

9. Clique em Salvar.

Editar ou copiar diretivas de backup

O CA ARCserve Central Host-Based VM Backup permite editar e copiar as diretivas de backup do CA ARCserve D2D depois de serem criadas.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Clique em Diretivas na barra de navegação para abrir a tela Diretivas.

2. Na tela Diretivas, clique na caixa de seleção ao lado de uma diretiva e execute uma das seguintes ações:

   - Clique em Editar na barra de ferramentas e edite a diretiva selecionada.
   - Clique em Copiar na barra de ferramentas para copiar e criar uma nova diretiva a partir da diretiva selecionada.

     Observação: ao copiar uma diretiva, a caixa de diálogo Copiar diretiva é aberta. Especifique um nome para o nova diretiva e clique em OK.

   A caixa de diálogo Editar diretiva é aberta.

3. Se desejar alterar o nome da diretiva, especifique um nome no campo Nome da diretiva.

4. Na guia Configurações de backup, clique em Configurações de proteção e especifique as seguintes informações:

   - **Destino do backup**--especifique uma pasta compartilhada remota na qual deseja salvar suas sessões de backup.
   - **Proxy de backup de VM do CA ARCserve D2D--**especifique o nome do host ou endereço IP do servidor em que o CA ARCserve D2D foi instalado. Se o CA ARCserve D2D ainda não estiver instalado, você poderá usar o CA ARCserve Central Protection Manager para implantá-lo. Forneça as credenciais apropriadas ao servidor. O número de porta padrão é 8014. Se tiver alterado esse padrão durante a instalação do CA ARCserve D2D, especifique o número de porta correto.
   - **Configuração de retenção** -- é possível definir a diretiva de retenção com base no número de pontos de recuperação a serem retidos (mescla sessões) ou com base no número de conjuntos de recuperação a serem retidos (exclui conjuntos de recuperação e desativa os itens incrementais ininterruptos). A opção padrão é Reter pontos de recuperação. Para obter mais detalhes, consulte Especificar configurações de proteção, no Guia do Usuário do CA ARCserve Central Protection Manager.
   - **Compactação** - selecione um nível de compactação. O valor padrão é Padrão. É possível especificar a opção Sem compactação ou Compactação máxima.
   - **Criptografia** - escolha um nível de criptografia. O valor padrão é Sem criptografia. Se escolher um nível de criptografia, você deverá fornecer uma senha criptografada, usada para restaurar dados criptografados.
   - **Acelerador de backup** - digite a taxa em que os backups são gravados em disco. Diminua essa taxa para reduzir a carga da CPU ou de rede, mas observe que isso aumenta a janela de backup. Esta opção é ativada, por padrão.

5. Clique em Programar e preencha as seguintes informações:

   - **Data e hora de início**-- especifique a data e a hora em que deseja iniciar as tarefas de backup.
   - **Backup incremental** - defina uma programação repetida para as tarefas de backup incremental. O valor padrão é repetir os backups incrementais uma vez por dia.
   - **Backup completo** - defina uma programação repetida para as tarefas de backup completo. Por padrão, o valor é definido para Nunca se repetir.
   - **Backup de verificação** - defina uma programação de repetição para as tarefas de backup de verificação. Por padrão, o valor é definido para Nunca se repetir.

6. Clique em Avançado e preencha as seguintes informações:

   - **Truncar log** - ative as seguintes opções se desejar truncar os arquivos de log do aplicativo:

     - **SQL Server** - escolha uma programação de truncamento diária, semanal ou mensal.

     - **Exchange Server** - escolha uma programação de truncamento diária, semanal ou mensal.

   - **Reservar espaço no destino** - especifique a porcentagem de espaço a ser reservado para a execução de um backup. Essa quantidade de espaço contínuo é, então, imediatamente reservada no destino antes que o backup comece a gravar os dados, e ajuda a acelerar o backup.

   - **Catálogos** - selecione a opção Gerar catálogo do sistema de arquivos para agilizar a pesquisa depois de cada backup para reduzir o tempo de espera de pesquisa do navegador.

     Se essa opção não estiver selecionada, as restaurações poderão ser executadas imediatamente após o backup sem precisar esperar até que a tarefa seja concluída. Por padrão, essa opção está desativada.

     Observação: gerar um catálogo do sistema de arquivos para cada tarefa de backup resulta em uma maior quantidade de armazenamento em disco necessária para armazenar os arquivos de metadados e os arquivos de catálogos e um aumento no uso da CPU. Além disso, se a origem do backup contiver vários arquivos, o processo de geração de um catálogo pode ser uma tarefa demorada.

     Observação: se você tiver selecionado uma ReFS ou um volume NTFS de redução de redundância como a origem do backup, um catálogo não poderá ser gerado e uma mensagem de aviso será exibida informando sobre essa condição.

7. Clique em Configurações de backup anterior ou posterior e especifique os comandos de backup anterior ou posterior necessários. Se necessário, forneça as credenciais corretas:
   - **Executar um comando antes do início do backup** - digite o comando de script a ser executado antes do início da tarefa de backup.
   - **No código de saída**-- ative essa opção para disparar o comando de script em um código de saída específico.
   - **Executar tarefa** - caso selecionada, o software continuará executando a tarefa se o código de saída especificado for retornado.
   - **Cancelar tarefa** - caso selecionada, o software anulará a tarefa se o código de saída especificado for retornado.
   - **Executar um comando depois de gerar um instantâneo** - digite o comando de script a ser executado depois que o instantâneo for gerado.
   - **Executar um comando quando o backup terminar** - digite o comando de script a ser executado depois que o backup for concluído.
8. (Opcional) Clique na guia Preferências. Configure os alertas por email desejados, conforme a necessidade. Se ativar essas opções, clique em Configurações de email para configurar o servidor de email.
9. Clique em Salvar.

A diretiva é editada ou copiada.

Atribuir e remover a atribuição de nós de diretivas de backup

Para proteger várias máquinas virtuais, selecione a diretiva que deseja usar e atribua-a a um ou mais nós.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Clique em Diretivas na barra de navegação para abrir a tela Diretivas.
2. Na tela Diretivas, clique na guia Atribuição de diretiva.
3. Na lista Diretivas, selecione a diretiva que deseja atribuir.

   Clique em Atribuir e remover atribuição para abrir a caixa de diálogo Atribuir/Remover atribuição de diretiva.

4. Especifique os seguintes campos da caixa de diálogo Atribuir/remover a atribuição de diretivas:

   - **Grupo--**permite selecionar o nome do grupo que contém os nós que deseja atribuir.
   - **Filtro Nome do nó--**permite filtrar os nós disponíveis com base em critérios comuns.

     Observação: o campo Nome do nó permite filtrar nós usando caracteres curinga.

     Por exemplo, usar o Acc* permite filtrar todos os nós com um nome de nó que comece com Acc. Para limpar os resultados do filtro, clique em X no campo Filtro.

5. Execute uma das seguintes ações:

   - **Atribuir nós a diretivas--**selecione os nós que deseja adicionar e clique na seta à direita.

     Os nós são movidos da lista Nós disponíveis para a lista Nós selecionados.

     Observação: para selecionar e mover todos os nós, clique na seta dupla à direita.

   - **Remover a atribuição de nós de diretivas**--selecione os nós que deseja remover a atribuição e clique na seta à esquerda.

     Os nós são movidos da lista Nós selecionados para a lista Nós disponíveis.

     Observação: para selecionar e mover todos os nós, clique na seta dupla à esquerda.

   Clique em OK.

6. Se necessário, forneça um nome de usuário global e a senha e aplique-os aos nós selecionados.

   Clique em OK.

   Os nós selecionados são adicionados à lista Atribuição de diretiva, com o status da implantação [Atribuído] pendente.

   Observação: é possível também visualizar o status da implantação na tela Nó.

7. Clique na opção Implantar agora para aplicar a diretiva atribuída aos nós especificados imediatamente. Use o botão Atualizar para atualizar o status.

Na tela Nó, o status dos nós especificados na lista Atribuição de diretiva mostra agora a diretiva atribuída na coluna Diretiva. Clique no Nome do nó e selecione Efetuar logon no D2D para verificar o status das tarefas de backup.

Exibir logs do CA ARCserve Central Host-Based VM Backup

O Log de exibição contém informações abrangentes sobre todas as operações executadas pelo aplicativo. O log fornece uma trilha de auditoria de todas as tarefas executadas (com as atividades mais recentes listadas primeiro) e pode ser útil para a solução dos problemas que podem ocorrer.

Siga estas etapas:

1. Na página inicial, clique em Exibir logs na barra de navegação.

   A tela Exibir logs é exibida.

2. Nas listas suspensas, especifique as informações de log que você deseja exibir.

   - **Gravidade -** essa opção permite especificar a gravidade do log que você deseja exibir. É possível especificar as seguintes opções de gravidade:

     - **Todos -** essa opção permite exibir todos os logs, independentemente da gravidade.
     - **Informações -** essa opção permite exibir apenas os logs que descrevem informações gerais.
     - **Erros -** essa opção permite exibir apenas os logs que descrevem erros graves que ocorreram.
     - **Avisos -** essa opção permite exibir apenas os logs que descrevem avisos de erros que ocorreram.
     - **Erros e avisos -** essa opção permite exibir apenas erros graves e avisos de erros que ocorreram.

- **Módulo -** essa opção permite especificar o módulo para o qual você deseja exibir logs. É possível especificar as seguintes opções de módulo:
  - **Todos -** essa opção permite exibir os logs sobre todos os componentes do aplicativo.
  - **Comum -** essa opção permite exibir os logs sobre processos comuns.
  - **Importar nós a partir da detecção** – essa opção permite exibir os logs sobre nós que foram importados somente a partir da detecção automática.
  - **Importar nós do Hypervisor** - essa opção permite exibir os logs sobre nós que foram importados somente a partir do Hypervisor.
  - **Gerenciamento de diretivas -** essa opção permite exibir apenas os logs sobre gerenciamento de diretivas.
  - **Atualizações** - essa opção permite exibir apenas os logs sobre a atualização do aplicativo.
  - **Verificação prévia** - essa opção permite exibir apenas os logs que executaram o status de verificação prévia em cada nó.
  - **Enviar tarefas de backup da VM** – essa opção permite exibir apenas os logs em que os nós foram enviados para tarefas de backup da máquina virtual.
  - **Atualizar vários nós** - essa opção permite exibir apenas os logs de atualização de vários nós ao mesmo tempo.
  - **Tarefa de mesclagem do CA ARCserve D2D** - essa opção permite exibir apenas os logs de tarefas de mesclagem do CA ARCserve D2D.
- **Nome do nó** - essa opção permite exibir apenas os logs de um determinado nó.

  Observação: esse campo suporta os caracteres curinga '*' e '?'. Por exemplo, digite 'lod*' para retornar todos os logs de atividades para o nome de computador iniciado por 'lod'.

Observação: as opções de Gravidade, Módulo e Nome do nó podem ser aplicadas em grupo. Por exemplo, é possível exibir erros (gravidade) que estão relacionados a atualizações (Módulo) para o nó X (Nome do nó).

Os logs são exibidos com base nas opções de exibição especificadas.

Observação: a hora exibida no log é baseada no fuso horário do servidor de banco de dados do aplicativo.

Exibir informações do log de atividades de um nó específico

O CA ARCserve Central Host-Based VM Backup permite exibir informações do log de atividades de um determinado nó do CA ARCserve D2D. Este log fornece uma trilha de auditoria de todas as tarefas executadas (com as atividades mais recentes relacionadas primeiro) e pode ser útil para a solução dos problemas que podem ocorrer.

Para exibir informações do log de atividades de um nó específico

1. Abra o aplicativo e clique em Nó na Barra de navegação.

   A tela Nó é exibida.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

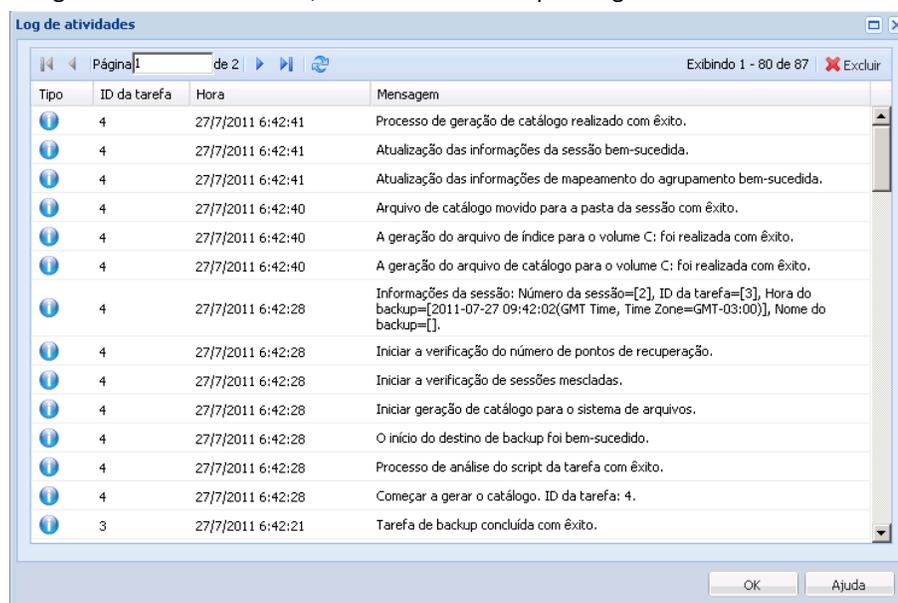
   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Procure e clique no nó que deseja efetuar logon e, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   O CA ARCserve D2D abre e você é conectado à página inicial do nó do CA ARCserve D2D.

   Observação: se uma nova janela do navegador não for aberta, verifique se as opções de pop-up de seu navegador permitem todos os pop-ups ou pop-ups somente para este site.

4. Clique em Exibir logs na lista Tarefas.

   O log de atividades é aberto, conforme ilustrado pela seguinte:

   O Log de atividades fornece as seguintes informações:

   - **Tipo--**especifica a gravidade da atividade, que inclui informações, avisos e erros.
   - **ID da tarefa--**especifica a tarefa a qual a atividade se aplica.
   - **Tempo--**especifica a data e a hora a qual a atividade se aplica.
   - **Mensagem--**descreve a atividade.

5. Clique em OK para fechar a caixa de diálogo Log de atividades.

Exibir o status do CA ARCserve Central Host-Based VM Backup em um relatório

Se você instalou o CA ARCserve Central Protection Manager e o CA ARCserve Central Reporting, é possível adicionar o servidor proxy de backup da VM com base em host ao CA ARCserve Central Protection Manager e, em seguida, gerar o relatório de status da proteção da virtualização para exibir o status do seu proxy.

Para obter mais detalhes sobre o relatório de status da proteção da virtualização, consulte o Guia do Usuário do CA ARCserve Central Reporting.

Adicionar links à barra de navegação

Cada CA ARCserve Central Applications possui um link Adicionar nova guia na barra de navegação. Use este recurso para adicionar entradas na barra de navegação para outros aplicativos da web que deseja gerenciar. No entanto, para cada aplicativo instalado, um novo link é automaticamente adicionado à barra de navegação. Por exemplo, se você tiver instalado o CA ARCserve Central Reporting e o CA ARCserve Central Virtual Standby no "computador A" e, em seguida, iniciar o CA ARCserve Central Reporting, o CA ARCserve Central Virtual Standby é automaticamente adicionado à barra de navegação.

Observação: cada aplicativo instalado é detectado somente se outros CA ARCserve Central Applications estiverem no mesmo computador.

Siga estas etapas:

1. Na barra de navegação do aplicativo, clique no link Adicionar nova guia.
2. Especifique o nome e o URL do aplicativo ou site que deseja adicionar. Por exemplo, www.google.com.

   Como opção, é possível especificar o local de um ícone.
3. Clique em OK.

   A nova guia é adicionada à parte inferior da barra de navegação.

Lembre-se das seguintes considerações:

- Para sua conveniência, o link do Suporte da CA é adicionado por padrão.

É possível remover a nova guia, destacando a guia e clicando no link Remover.

Considerações para proteger mapeamentos de dispositivos simples

Considere o seguinte comportamento ao proteger mapeamentos de dispositivos simples (rdm):

- O aplicativo não oferece suporte à proteção de mapeamentos de dispositivos simples no modo de compatibilidade física (discos desse tipo são dispositivos físicos). O aplicativo omite mapeamentos de dispositivos simples no modo de compatibilidade física da origem de backup durante o processo de backup. Uma solução para esse comportamento é instalar o CA ARCserve D2D no sistema operacional convidado e executar backups da mesma maneira como faria com discos físicos.

- O aplicativo oferece suporte à proteção de mapeamentos de dispositivos simples no modo de compatibilidade física. Porém, considere as seguintes limitações:
  - Em relação aos backups completos, o aplicativo permite o backup de discos RDM completos no modo de compatibilidade virtual. No entanto, se não for usada a compactação de dados, os conjuntos de dados de backup poderão ser do mesmo tamanho que o disco de origem.
  - O CA ARCserve Central Host-Based VM Backup restaura discos virtuais RDM no modo de compatibilidade como discos virtuais normais. Após o processo de recuperação, o disco não está mais configurado como nem se comporta como um disco virtual RDM.
  - Uma abordagem alternativa para o backup de RDMs virtuais do modo de compatibilidade é instalar o CA ARCserve D2D no sistema operacional convidado e fazer backup dos RDMs da mesma maneira como faria com computadores físicos.

Alterar o protocolo de comunicação do servidor

Por padrão, o CA ARCserve Central Applications usa o protocolo HTTP (Hypertext Transfer Protocol) para comunicação entre todos os seus componentes. Caso esteja preocupado com a segurança das senhas comunicadas entre esses componentes, é possível alterar o protocolo em uso para HTTPS (Hypertext Transfer Protocol Secure). Além disso, se você não precisar deste nível extra de segurança, é possível alterar o protocolo em uso para HTTP.

Siga estas etapas:

1. Efetue logon no computador no qual o aplicativo está instalado usando uma conta administrativa ou uma conta com privilégios administrativos.

   Observação: se não efetuar logon usando uma conta administrativa ou uma conta com privilégios administrativos, configure a linha de comando para ser executada usando o privilégio Run as Administrator.

2. Abra a linha de comando do Windows.

3. Siga um destes procedimentos:

   ■ **Para alterar o protocolo de HTTP para HTTPS:**

   Inicie a ferramenta de utilitário changeToHttps.bat no seguinte local padrão (o local da pasta BIN pode variar dependendo de onde você instalou o aplicativo):

   ```
   C:\Arquivos de Programas\CA\ARCserve Central Applications\BIN
   ```

   Quando o protocolo for alterado com êxito, a seguinte mensagem será exibida:

   ```
   O protocolo de comunicação foi alterado para HTTPS.
   ```

   ■ **Para alterar o protocolo de HTTPS para HTTP:**

   Inicie a ferramenta de utilitário changeToHttp.bat no seguinte local padrão (o local da pasta BIN pode variar dependendo de onde você instalou o aplicativo):

   ```
   C:\Arquivos de Programas\CA\ARCserve Central Applications\BIN
   ```

   Quando o protocolo for alterado com êxito, a seguinte mensagem será exibida:

   ```
   O protocolo de comunicação foi alterado para HTTP.
   ```

4. Reinicie o navegador e reconecte-se ao CA ARCserve Central Applications.

   Observação: quando você altera o protocolo para HTTPS, um aviso é exibido no navegador web. Esse comportamento ocorre devido a um certificado de segurança autoassinado que solicita que você ignore o aviso e continue ou adicione esse certificado ao navegador para evitar que o aviso seja exibido novamente.

Definir um modo de transporte para backups

É possível definir um modo de transporte específico (transferência de dados) a ser usado para tarefas de backup do D2D que executam usando o Host-Based VM Backup. Por padrão, o Host-based VM backup usa um modo que permite o Host-Based VM Backup otimizar o desempenho (aumentar a velocidade) da operação de backup. No entanto, quando você deseja especificar um modo de transporte específico para as operações de backup, é necessário configurar a chave de registro descrita neste tópico.

O Host-Based VM Backup pode executar backups usando os seguintes modos de transporte:

■ Modo de transporte HOTADD (na página 195)

■ Modo de transporte NBD (na página 195)

■ Modo de transporte NBDSSL (na página 195)

■ Modo de transporte SAN (na página 195)

Lembre-se das seguintes considerações:

- Esta tarefa de configuração é opcional. Por padrão, o Host-Based VM Backup executa backups usando um modo de transporte que otimiza o desempenho da operação de backup.
- Ao configurar esta chave de registro para usar um modo de transporte específico e o modo não está disponível, o Host-Based VM Backup usa um modo de transporte padrão disponível para a operação de backup.

Siga estas etapas:

1. Efetue logon no sistema de proxy de backup do CA ARCserve D2D para as máquinas virtuais.

   Abra o editor de registro do Windows e procure a seguinte chave de registro:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE
   D2D\AFBackupDll\{VM-InstanceUUID}].
   ```

2. Clique com o botão direito do mouse em VM-InstanceUUID, selecione Novo e clique em Valor da sequência de caracteres no menu pop-up.

   Nomeie o novo valor da sequência de caracteres, como a seguir:

   ```
   EnforceTransport
   ```

3. Clique com o botão direito em EnforceTransport e clique em Modificar no menu pop-up para abrir a caixa de diálogo Editar sequência.
4. No campo Dados de valor, especifique o modo de transporte que você deseja usar durante a tarefa de backup. Especifique um dos seguintes valores:

   hotadd

   Modo de transporte HOTADD (na página 195)

   nbd

   Modo de transporte NBD (na página 195)

   nbdssl

   Modo de transporte NBDSSL (na página 195)

   san

   Modo de transporte SAN (na página 195)

5. Clique em OK para aplicar o valor e fechar a caixa de diálogo Editar sequência.

O modo de transporte é definido e usado na próxima vez que uma tarefa for executada.

Capítulo 4: Restaurar e recuperar máquinas virtuais

As opções de restauração e recuperação disponíveis dependem de como o backup do sistema foi realizado. Por exemplo, não é possível usar sessões de backup criadas com o CA ARCserve Central Host-Based VM Backup para executar operações de restauração granular do Microsoft Exchange ou em nível de aplicativo, mas é possível executá-las usando sessões criadas com o CA ARCserve Central Protection Manager ou CA ARCserve D2D. Algumas opções de restauração disponíveis no CA ARCserve D2D podem não estar disponíveis neste aplicativo. Por exemplo, a opção Restaurar no local original não é possível em backups do aplicativo porque o local do servidor de proxy é diferente do local de origem do backup da máquina virtual.

Para obter mais informações, consulte o tópico Considerações sobre a restauração (na página 105) para ajudar a determinar quando usar os Métodos de restauração (na página 92) disponíveis.

Esta seção contém os seguintes tópicos:

Métodos de restauração

O modo como a sessão de backup foi criada determina quais métodos de restauração podem ser usados. Por exemplo, alguns métodos de restauração só são possíveis se executados com uma versão do CA ARCserve D2D instalada localmente. Outros métodos exigem que a máquina virtual esteja ligada na hora do backup.

Procurar pontos de recuperação (na página 93)

Permite procurar os pontos de recuperação disponíveis (backups bem-sucedidos) a partir de uma exibição de calendário. Use esse método para recuperar arquivos, pastas ou executar o processo de restauração de nível de aplicativo.

Os backups criados com o CA ARCserve D2D, o CA ARCserve Central Host-Based VM Backup ou o CA ARCserve Central Protection Manager podem ser restaurados com este método.

Localizar arquivos/pastas para restauração (na página 96)

Permite localizar arquivos ou pastas específicos a serem restaurados.

Os backups criados com o CA ARCserve D2D podem ser restaurados com este método. Ele também está disponível para restaurar backups criados com o CA ARCserve Central Host-Based VM Backup e o CA ARCserve Central Protection Manager quando a máquina virtual estiver ligada no momento do backup.

Recuperar VM (na página 99)

Permite procurar todos os pontos de recuperação de máquina virtual disponíveis (backups bem-sucedidos) a partir de uma exibição de calendário. Assim, é possível especificar a máquina virtual que deseja recuperar.

Esse método está disponível para restaurar backups criados com o CA ARCserve Central Host-Based VM Backup, provisionar uma máquina virtual e restaurar o sistema operacional, aplicativos e dados do ponto de recuperação especificado.

Restauração de aplicativo (na página 105)

Para restaurar um Microsoft Exchange ou SQL Server totalmente sem precisar recriá-los, clique no método Procurar pontos de recuperação a partir de uma versão do CA ARCserve D2D instalada localmente.

Recuperação bare metal (na página 155)

BMR (Bare Metal Recovery - Recuperação Bare Metal) é o processo de restauração de um computador a partir do estado bare metal, incluindo o sistema operacional, aplicativos de software, configurações e dados. A BMR requer se tenha uma imagem do Windows, um kit de inicialização e ao menos um backup completo. Os backups criados com o CA ARCserve D2D, o CA ARCserve Central Host-Based VM Backup, o CA ARCserve Central Virtual Standby e o CA ARCserve Central Protection Manager podem ser restaurados com este método. No entanto, se a máquina virtual foi desligada durante o backup, não será possível executar a BMR.

Restaurar de pontos de recuperação

O método de restauração Procurar pontos de recuperação permite localizar backups bem-sucedidos (chamados de pontos de recuperação) a partir de uma exibição de calendário. É possível procurar e selecionar o conteúdo do backup, incluindo os aplicativos que deseja restaurar. O procedimento de restauração com o método Procurar pontos de recuperação é o mesmo usado para o CA ARCserve D2D, com uma exceção. Não é possível usar a opção de restauração para o local original para restaurar os pontos de recuperação de máquinas virtuais.

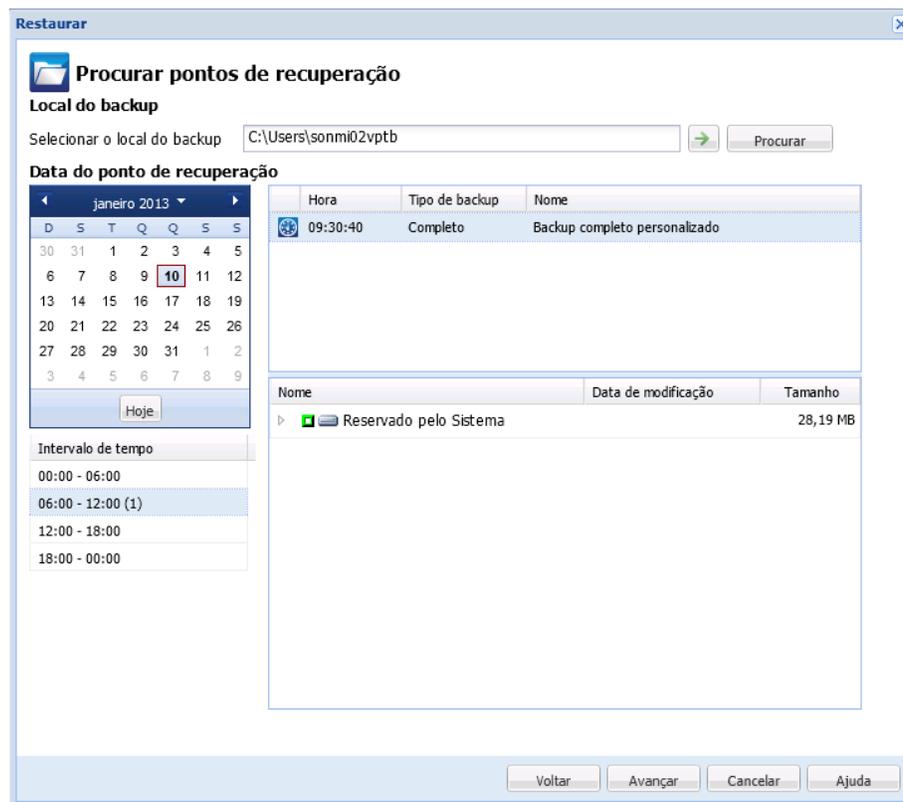
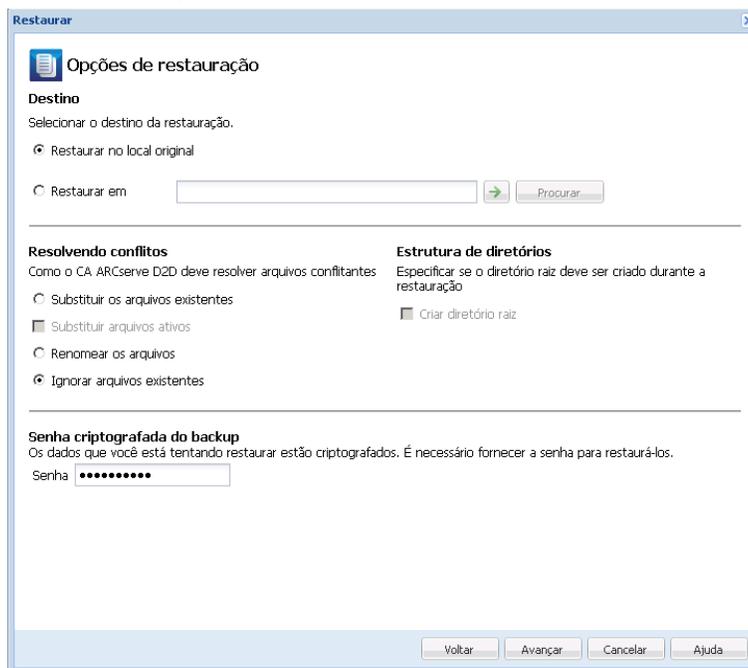
Siga estas etapas:

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.

   Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.

2. Na caixa de diálogo Restaurar, clique em Procurar pontos de recuperação.

   A caixa de diálogo Restaurar é exibida e o Local do backup é fornecido com base no nó selecionado. Se desejar, altere para outro destino de backup e forneça as credenciais de usuário.

3. Clique na data do ponto de recuperação e, em seguida, clique na hora do ponto de recuperação. Selecione o conteúdo que deseja restaurar. Selecione um volume, um arquivo, uma pasta, um banco de dados ou um aplicativo completo. Caixas verdes sólidas ao lado de uma seleção indicam que ele está selecionado para restauração. Clique em Avançar ao concluir.

4. Na caixa de diálogo Opções de restauração, especifique o destino da restauração.

   - **Restaurar no local original (desativar)--** para as sessões do CA ARCserve Central Host-Based VM Backup, não é possível restaurar para o local original. Para restaurar arquivos ou pastas para o local original no sistema operacional convidado de uma VM, é necessário instalar o CA ARCserve D2D no sistema operacional convidado da VM ou restaurar em uma pasta da rede que esteja compartilhada na VM.
   - **Restaurar em--** especifique o destino que em que deseja restaurar.
   - **Substituir arquivos existentes--**substitui os arquivos localizados no destino.
   - **Substituir os arquivos ativos--**substitui arquivos em uso ou sendo acessados na reinicialização.
   - **Renomear arquivos**--cria um novo arquivo se o nome de arquivo já existir. A seleção desta opção copia os arquivos de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados são restaurados para o arquivo com a nova extensão.
   - **Ignorar arquivos existentes -** ignora arquivos existentes e não substitui esses arquivos localizados no destino. Essa é a configuração padrão.
   - **Criar diretório raiz--**recria a mesma estrutura de diretório raiz no destino encontrado na imagem de backup.

5. Clique em Avançar. Na tela Resumo de restauração, verifique se todas as opções estão corretas. Caso contrário, clique em Voltar. Em caso afirmativo, clique em Concluir para iniciar o processo de restauração.

Restaurar por montagem de um ponto de recuperação

O método de restauração Montar ponto de recuperação permite montar um ponto de recuperação para o sistema de proxy de backup. Para montar um ponto de recuperação, você deve efetuar logon na interface do usuário do CA ARCserve D2D.

Siga estas etapas:

1. Efetue logon no CA ARCserve Central Host-Based VM Backup e clique em Nó na barra de navegação.
2. Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.

   Uma versão CA ARCserve Central Host-Based VM Backup do CA ARCserve D2D é exibida.

   Observação: verifique se as opções de pop-up do seu navegador permitem todos os pop-ups ou pop-ups apenas deste site, de modo que uma nova janela de navegador possa ser aberta.

Para obter mais detalhes sobre a caixa de diálogo Montar ponto de recuperação, clique em Ajuda na página inicial do CA ARCserve D2D.

Restaurar dados usando a opção Localizar arquivos/pastas para restauração

Sempre que o aplicativo executar um backup com êxito, todas as pastas ou arquivos armazenados em backup serão incluídos na imagem de instantâneo do seu backup. Este método de restauração permite especificar exatamente qual arquivo ou pasta deve ser restaurado.

Siga estas etapas:

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.

   Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.
2. Na caixa de diálogo Restaurar, clique em Localizar arquivos/pastas para restauração.
3. Na caixa de diálogo Localizar arquivos/pastas a ser restaurados, especifique ou navegue até o local do backup. Se estiver restaurando a partir de uma sessão do CA ARCserve Central Host-Based VM Backup, não será possível especificar um local de cópia de arquivo. A restauração de cópia de arquivo é permitida apenas se estiver restaurando a partir de sessões de backup do CA ARCserve Central Protection Manager ou do CA ARCserve D2D .

4. Especifique o nome de arquivo ou pasta para restaurar.

   Observação: o campo Nome de arquivo oferece suporte à pesquisa de nome completo e pesquisa com caracteres curinga. Se não souber o nome do arquivo completo, é possível simplificar os resultados da pesquisa especificando os caracteres curinga "*" e "?" no campo Nome de arquivo.

   Os caracteres curinga suportados para o nome de arquivo ou pasta são os seguintes:

   - "*" - use o asterisco para substituir zero ou mais caracteres em um nome de arquivo ou diretório.
   - "?" - use o ponto de interrogação para substituir um único caractere em um nome de arquivo ou pasta.

   Por exemplo, se *.txt for especificado, todos os arquivos com uma extensão de arquivo .txt serão exibidos nos resultados da pesquisa.

5. (Opcional) Especifique um nome de caminho para refinar sua pesquisa e selecione se deseja incluir ou não subdiretórios ou arquivos e pastas.

6. Clique em Localizar para iniciar a pesquisa.

   Os resultados da pesquisa são exibidos. Se a pesquisa detectar várias ocorrências (pontos de recuperação) do mesmo arquivo pesquisado, ela listará todas as ocorrências classificadas por data (com a mais recente listada primeiro).

7. Selecione a versão que deseja restaurar da lista e clique em Avançar.

   A caixa de diálogo Opções de restauração é exibida. É possível restaurar apenas em um local alternativo. Especifique ou procure o local onde deseja armazenar a imagem de backup. Clique na seta verde para verificar a conexão. Forneça as credenciais do usuário, se necessário.

8. Selecione as opções de resolução de conflito:

   Substituir arquivos existentes

   Substitui (sobrescreve) qualquer arquivo localizado no destino da restauração. Todos os objetos serão restaurados dos arquivos de backup, independentemente da presença atual deles no computador.

   Substituir os arquivos ativos

   Substitui todos os arquivos ativos ao reinicializar. Se, durante a tentativa de restauração, o software detectar que o arquivo existente está atualmente em uso ou sendo acessado, ele não substituirá o arquivo imediatamente, mas evitará que qualquer problema atrase a substituição dos arquivos ativos até a próxima reinicialização do computador. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a próxima reinicialização).

   Observação: se essa opção não estiver selecionada, os arquivos ativos serão ignorados na restauração.

   Renomear arquivos

   Cria um novo arquivo se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão restaurados no novo arquivo.

   Ignorar arquivos existentes

   Ignora e não substitui (sobrescreve) os arquivos existentes localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

   Por padrão, esta opção está ativada.

9. (Opcional) Selecione Criar diretório raiz em Estrutura de diretórios.

   Esta opção recria a mesma estrutura de diretórios raiz no caminho de destino da restauração.

   Observação: se essa opção não for selecionada, o arquivo ou pasta será restaurado diretamente para a pasta de destino.

10. Digite a senha de criptografia de backup para restaurar os dados criptografados e, em seguida, clique em Avançar.

    A caixa de diálogo Resumo da restauração é exibida.

11. Examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.

    - Se as informações de resumo não estiverem corretas, clique em Anterior e volte à caixa de diálogo em questão para alterar a configuração incorreta.
    - Se as informações de resumo estiverem corretas, clique em Concluir para iniciar o processo de restauração.

Recuperar uma máquina virtual inteira

É possível recuperar uma máquina virtual inteira a partir de uma sessão do CA ARCserve Central Host-Based VM Backup.

Este método de backup é como executar uma BMR. Com esse método, é possível recuperar o sistema operacional convidado do Windows, os aplicativos e os dados.

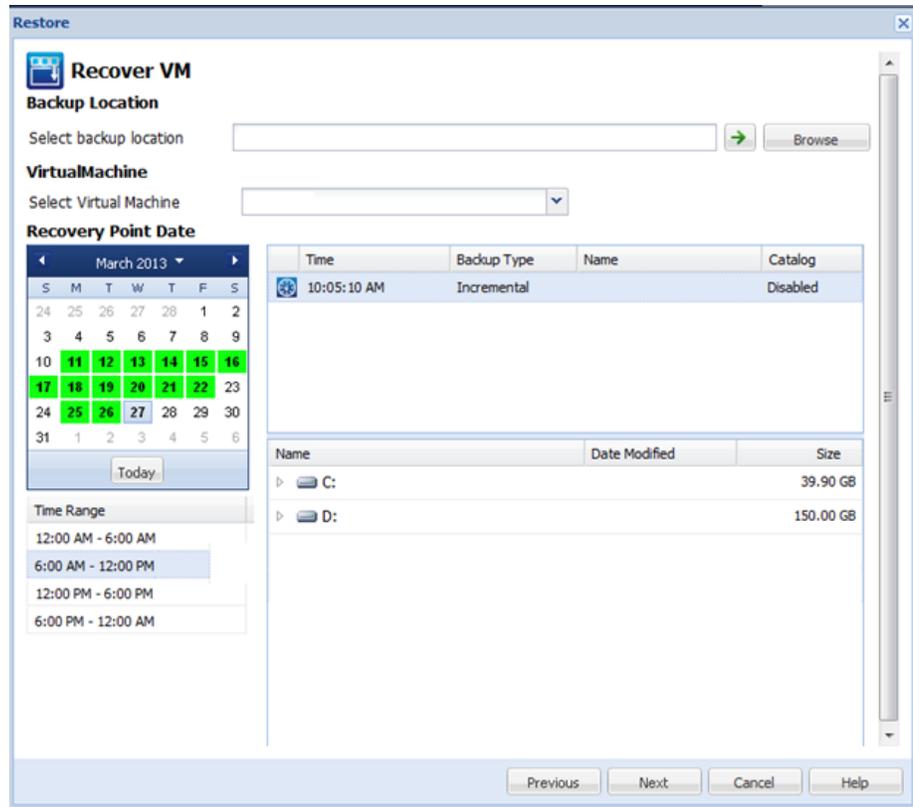
Siga estas etapas:

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.

   Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas. O aplicativo registra-o no CA ARCserve D2D.

2. Na caixa de diálogo Restaurar, clique em Recuperar VM.

3. A caixa de diálogo Restaurar é exibida. Os campos Local do backup e Máquina virtual são preenchidos com base na VM selecionada na tela Nó. Se desejar, altere esses valores.

Especifique a origem onde as sessões de backup de máquinas virtuais serão armazenadas. Digite as credenciais do usuário, se solicitado.

O menu suspenso lista todas as máquinas virtuais no local no campo Backup Location.

4. No calendário, clique na data da imagem da máquina virtual que deseja recuperar. Na lista Time Range, clique na imagem de backup a ser recuperada. O conteúdo que corresponde a sua seleção é exibido para sua referência. Não é possível selecionar volumes individuais, pastas ou arquivos. A máquina virtual inteira é restaurada.

5. Clique em Avançar. Na caixa de diálogo Opções de restauração, especifique o destino da restauração.

   Restaurar no local original

   Restaura a máquina virtual no local original a partir do qual a imagem de backup foi capturada. Por padrão, esta opção está ativada.

   Para obter mais informações, consulte o tópico Restaurar a VM no local original (na página 101).

   Restaurar em um local diferente

   Restaura a máquina virtual em outro local de onde a imagem de backup foi capturada.

   Para obter mais informações, consulte o tópico Restaurar a VM em um local diferente (na página 102).

6. Especifique as opções de resolução de conflito e após a recuperação. Por padrão, essas opções não são selecionadas.
   - Substituir a máquina virtual existente--substitui qualquer imagem da máquina virtual existente no servidor vCenter/ESX.
   - Ligar a máquina virtual--inicia a máquina virtual após a conclusão do processo de restauração.

7. Clique em Avançar. Digite as credenciais do vCenter/ESX Server para a origem do backup, se solicitado e clique em OK.

8. Na caixa de diálogo Resumo da restauração, verifique se todas as opções estão corretas. Caso contrário, clique em Voltar. Em caso afirmativo, clique em Concluir para iniciar o processo de restauração.

Restaurar máquinas virtuais aos locais originais

Durante o processo de configuração para restaurar a VM, é necessário selecionar a opção de onde deseja restaurá-la. As seleções disponíveis são Restaurar no local original e Restaurar em um local diferente.

Se selecionar restaurar a VM no local original, execute as seguintes etapas:

Siga estas etapas:

1. Na caixa de diálogo Opções de restauração, após especificar as opções Resolver conflitos e Após a recuperação, selecione Restaurar para o local original e clique em Avançar.

   Observação: para obter mais informações sobre as opções Resolver conflitos e Após a recuperação, consulte o tópico Restaurar dados de máquinas virtuais.

   A caixa de diálogo Definir credencial para a origem vCenter/ESX Server é exibida.

2. Especifique as credenciais para acessar a máquina virtual.
   - **vCenter/ESX Server--**especifique o nome do host ou endereço IP de destino do sistema vCenter ou ESX Server.
   - **Nome da VM--**especifique o nome de host da máquina virtual que você está restaurando.
   - **Protocolo--**especifique o protocolo que deseja usar para a comunicação com o servidor de destino. As seleções disponíveis são HTTP e HTTPS.
   - **Número da porta--**especifique a porta que deseja usar para a transferência de dados entre o servidor de origem e o destino. Por padrão, este número da porta é 443.
   - **Nome de usuário**--especifique o nome de usuário com permissão de acesso para efetuar logon na máquina virtual que você está restaurando.
   - **Senha--**especifique a senha correspondente para o nome de usuário necessária para fazer logon na máquina virtual que está restaurando.
3. Quando as credenciais forem especificadas, clique em OK.

   A caixa de diálogo Resumo de restauração é exibida.
4. Examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.
   - Se as informações de resumo não estiverem corretas, clique em Anterior e volte à caixa de diálogo em questão para alterar a configuração incorreta.
   - Se as informações de resumo estiverem corretas, clique em Concluir para iniciar o processo de restauração.

Restaurar máquinas virtuais para locais diferentes

Durante o processo de configuração para restaurar a VM, é necessário selecionar a opção de onde deseja restaurá-la. As seleções disponíveis são Restaurar no local original e Restaurar em um local diferente.

Se desejar restaurar a máquina virtual em um local alternativo, execute as seguintes etapas:

Siga estas etapas:

1. Na caixa de diálogo Opções de restauração, após marcar as opções Resolver conflitos e Após a recuperação, selecione Restaurar em um local diferente.

   Observação: para obter mais informações sobre as opções Resolver conflitos e Após a recuperação, consulte o tópico Recuperar dados em máquinas virtuais.

   A caixa de diálogo Opções de restauração se expande para exibir restauração adicional em opções diferentes.

2. Especifique as informações do vCenter/ESX Server.

   - **vCenter/ESX Server--**especifique o nome do host ou endereço IP de destino do sistema vCenter ou ESX Server.
   - **Nome de usuário**--especifique o nome de usuário com permissão de acesso para efetuar logon na máquina virtual que estiver restaurando.
   - **Senha--**especifique a senha correspondente para o nome de usuário necessária para fazer logon na máquina virtual que está restaurando.
   - **Protocolo--**especifique o protocolo que deseja usar para a comunicação com o servidor de destino. As seleções disponíveis são HTTP e HTTPS.
   - **Número da porta--**especifique a porta que deseja usar para a transferência de dados entre o servidor de origem e o destino. Por padrão, este número da porta é 44.

3. Quando as informações do vCenter/ESX Server estiverem especificadas, clique no botão Estabelecer conexão com esse vCenter/ESX Server.

   Se as informações de credenciais de acesso ao servidor alternativo estiverem corretas, os campos Outras informações ficarão ativados.

4. Especificar outras informações.
   - **Nome da VM--**especifique o nome de host da máquina virtual que você está restaurando.
   - **ESX Server--**especifique o servidor ESX de destino. O menu suspenso contém uma lista de todos os servidores ESX associados à máquina virtual especificada.
   - **Pool de recursos--**selecione o pool de recursos ou pool de vApp que deseja usar para a recuperação da VM. Clique no botão Procurar pool de recursos para exibir a caixa de diálogo Selecionar um pool de recursos. Essa caixa de diálogo contém uma lista de todos os pools de recursos e pools de vApp disponível para o destino do servidor ESX. Selecione o pool a ser usado para a recuperação da máquina virtual. Você pode deixar este campo em branco se não quiser atribuir um pool de recursos ou de vApp à recuperação dessa máquina virtual.

     Observação: um pool de recursos é uma coleção configurada de recursos de CPU e memória. Um pool de vApp é uma coleção de uma ou mais máquinas virtuais que podem ser gerenciadas como um único objeto.
   - **Armazenamento de dados da VM--**Especifique o armazenamento de dados da VM de destino para a recuperação de máquina virtual ou cada disco virtual da máquina virtual.

     Uma máquina virtual pode ter vários discos virtuais e é possível especificar outro armazenamento de dados para cada disco virtual.

     Por exemplo:
     - Disk0 pode ser restaurado no Datastore1.
     - Disk1 pode ser restaurado no Datastore1.
     - Disk2 pode ser restaurado no Datastore2.

     Importante: para o Armazenamento de dados da VM, este campo será preenchido apenas se o usuário tiver permissões de administrador completas no sistema VMware. Se o usuário não tiver as permissões de administrador adequadas, o CA ARCserve Central Host-Based VM Backup continuará o processo de restauração depois que se conectar ao vCenter/ESX Server.
5. Quando outras informações forem especificadas, clique em Avançar.

   A caixa de diálogo Resumo de restauração é exibida.
6. Examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.
   - Se as informações de resumo não estiverem corretas, clique em Anterior e volte à caixa de diálogo em questão para alterar a configuração incorreta.
   - Se as informações de resumo estiverem corretas, clique em Concluir para iniciar o processo de restauração.

Considerações sobre a restauração

Use a tabela a seguir para determinar qual método de restauração usar nas condições relacionadas.

Método de restauração:	Quando desejar:	Considerações:
Procurar pontos de recuperação (use este método para executar restaurações de nível de aplicativo). Localizar arquivos/pastas para restauração	Restaurar um arquivo, uma pasta, um banco de dados ou um aplicativo que agora está corrompido.	■ **CA ARCserve Central Host-Based VM Backup**: para restaurar arquivos ou pastas, a VM deve estar ligada no momento do backup. Não é possível restaurar para o local original. Mapear um drive de rede no local original ou acessá-lo como um compartilhamento e restaurá-lo no local mapeado ou compartilhado. Instalar o CA ARCserve D2D no sistema operacional convidado de uma nova VM e restaurar um banco de dados do aplicativo. Para obter mais informações, consulte o tópico Restaurações em nível de aplicativo. ■ **CA ARCserve D2D ou CA ARCserve Central Protection Manager**: consulte o Guia do Usuário do Aplicativo.
Recuperar VM	Fornecer uma nova máquina virtual e restaurar o sistema operacional, aplicativos e dados	■ **CA ARCserve Central Host-Based VM Backup**: recomendado ■ **CA ARCserve D2D ou CA ARCserve Central Protection Manager**: não suportado

Também é possível usar os processos de recuperação bare metal e de restauração de nível de aplicativo. Para obter mais informações, consulte o tópico Métodos de restauração. (na página 92)

Restaurações em nível de aplicativo

O CA ARCserve Central Applications permite proteger e recuperar os dados, mas também ajuda a obter os aplicativos que usam dados de backup e em execução. As restaurações de nível de aplicativo usam o método de restauração Procurar pontos de recuperação. 'Durante o processo de restauração de nível de aplicativo, é possível recuperar o Microsoft Exchange ou SQL Server sem ter que executar uma recuperação de falhas completa.

Antes de iniciar o processo de restauração de nível de aplicativo, talvez seja necessário executar as seguintes tarefas:

- Fornecer uma nova máquina virtual com um sistema operacional convidado do Windows
- Instalar o CA ARCserve D2D no sistema operacional convidado.
- Para as operações de restauração do aplicativo do Exchange Server:
  - Verifique se a conta tem privilégios de função de Administrador total do Exchange para o Exchange Server 2003, ou privilégios de função de Administrador da organização do Exchange ou Administrador do servidor para o Exchange Server 2007/2010/2013.
  - Ao restaurar os bancos de dados do Exchange Server 2007 para grupos de armazenamento de recuperação, crie os grupos de armazenamento de recuperação no servidor protegido. De forma semelhante, quando estiver restaurando bancos de dados do Exchange Server 2010 ou 2013 em bancos de dados de recuperação, crie os bancos de dados de recuperação no servidor protegido.
  - Verifique o procedimento completo sobre como executar uma restauração, fornecido no Guia do Usuário do CA ARCserve D2D.

Restaurar dados do Exchange Server

Você pode executar restaurações em nível de aplicativo dos dados do Microsoft Exchange Server com o seguinte:

- Exchange Server 2003: ambiente de servidor único. O ambiente de agrupamento não é suportado.
- Exchange Server 2007: ambiente de servidor único, ambiente LCR (Local Continuous Replication - Replicação Contínua Local) e CCR (Cluster Continuous Replication - Replicação Contínua em Agrupamento). Para o Exchange Server 2007 CCR, instale o CA ARCserve D2D localmente nos nós ativo e passivo. É possível executar operações de backup de um nó ativo ou passivo, mas é possível realizar operações de restauração apenas no nó ativo. A SCC (Single Copy Cluster) não é suportada.
- Exchange Server 2010: ambiente de servidor único e ambiente DAG (Database Availability Group - Grupo de Disponibilidade do Banco de Dados). Para um ambiente DAG, verifique se o CA ARCserve D2D está instalado em todos os servidores no DAG. As operações de backup também podem ser executadas a partir de qualquer servidor para cópias de bancos de dados ativas e passivas, contudo, a restauração só pode ser realizada para uma cópia de banco de dados ativa.
- Exchange Server 2013: há suporte para backup e restauração do VSS (Volume Shadow Copy Service – Serviço de Cópia de Sombra de Volume) da Microsoft. A GRT (Granular Recovery Technology - Tecnologia de Recuperação Granular) não é suportada.

É possível restaurar os dados do Microsoft Exchange Server para os seguintes níveis:

- Nível do gravador do Microsoft Exchange: restaura todos os dados do Exchange Server.
- Nível do grupo de armazenamento: restaura um grupo de armazenamento específico (não se aplica ao Microsoft Exchange Server 2010).
- Nível de armazenamento de caixa de correio: restaura um armazenamento de caixa de correio específico (aplica-se somente ao Microsoft Exchange Server 2003).
- Nível do banco de dados de caixa de correio: restaura um banco da dados de caixa de correio específico (aplica-se ao Exchange Server 2007 e 2010).

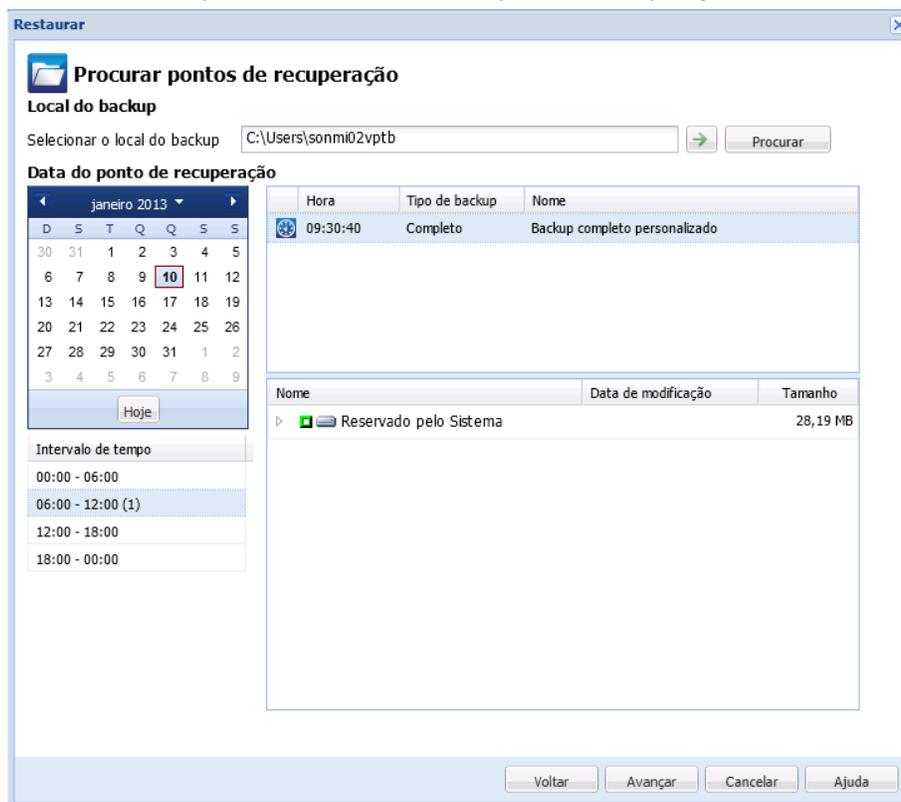
Observação: antes de começar, execute os pré-requisitos necessários em Restaurações em nível de aplicativo (na página 105).

Importante: A restauração de itens da caixa de correio do usuário do Microsoft Exchange Server não oferece suporte às sessões do CA ARCserve Central Host-Based VM Backup. Para restaurar os dados do Microsoft Exchange Server em um nível granular, faça backup dos dados do Exchange Server usando o CA ARCserve Central Protection Manager ou o CA ARCserve D2D.

Para restaurar dados do Exchange Server

1. Verifique se o CA ARCserve D2D está instalado no sistema operacional convidado.
2. Efetue logon no sistema operacional convidado da máquina virtual em que deseja fazer a restauração de dados do Exchange Server.
3. Inicie o CA ARCserve D2D e, em seguida, clique em Restaurar no painel de navegação do CA ARCserve D2D para abrir a caixa de diálogo Restaurar.
4. Clique em Procurar pontos de recuperação para abrir a caixa de diálogo Procurar pontos de recuperação.
5. No campo Selecionar local de backup na caixa de diálogo Procurar pontos de recuperação, especifique o caminho para a sessão de backup na máquina virtual do Host-Based VM Backup da qual deseja restaurar os dados do Exchange Server. O caminho a seguir é um exemplo do caminho para a sessão de backup na máquina virtual do Host-Based VM Backup:

   ```
   https://<nome do servidor>/<nome do compartilhamento> /vm@<nome do host ou
   endereço IP do sistema ESX Server>
   ```

6. No calendário, clique em uma data e hora do ponto de recuperação.

7. Clique em Avançar para abrir a caixa de diálogo Opções de restauração.

8. Selecione o destino da restauração.

   As opções disponíveis permitem restaurar no local original do backup, restaurar apenas o arquivo de despejo ou restaurar em um Grupo de armazenamento de recuperação/Banco de dados de caixa de correio de recuperação.

   Restaurar no local original

   Restaura no local original a partir do qual a imagem de backup foi capturada.

   Apenas arquivo de despejo

   Restaura apenas os arquivos de despejo.

   Para esta opção, o CA ARCserve D2D irá restaurar o arquivo do banco de dados do Microsoft Exchange em uma pasta especificada, e não o colocará online após a recuperação. É possível mover este arquivo em um servidor diferente e montá-lo manualmente no Exchange Server para exibir os dados contidos nele.

   Observação: quando há um Banco de dados de caixa de correio de recuperação, há falha na restauração que usar a opção Apenas arquivo de despejo.

Reproduzir log no banco de dados

Especifica que, quando os arquivos do banco de dados forem despejados na pasta de destino, é possível reproduzir e aplicar todos os arquivos de log de transações do Microsoft Exchange e confirmá-los no arquivo do banco de dados. Na próxima vez em que o banco de dados for iniciado, e os arquivos de log de transações que ainda não tiverem sido gravados nos arquivos do banco de dados forem, então, aplicados antes de o banco de dados tornar-se novamente disponível para você.

Observação: essa opção não se aplica ao Microsoft Exchange Server 2003

Restaurar no grupo de armazenamento para recuperação (Exchange 2007)

Restaura o banco de dados em um RSG (Recovery Storage Group - Grupo de armazenamento para recuperação).

Um RSG é um grupo de armazenamento que pode ser usado para fins de recuperação. É possível restaurar um banco de dados da caixa de correio do Microsoft Exchange a partir de um backup em um Grupo de armazenamento para recuperação e, em seguida, recuperar e extrair seus dados, sem afetar o banco de dados de produção que estiver sendo acessado por usuários finais.

- Se um único grupo de armazenamento ou banco de dados (exceto em um banco de dados de pasta pública) do mesmo grupo de armazenamento estiverem selecionados para restauração, o destino de restauração padrão é "Restaurar no grupo de armazenamento para recuperação" (ou "Restaurar para banco de dados de recuperação").
- Se vários grupos de armazenamento ou bancos de dados de vários grupos de armazenamento forem selecionados para restauração, o Exchange só pode ser restaurado no local original ou ser restaurado com a opção "Apenas arquivo de despejo". O destino de restauração padrão é Restaurar no local original.

Antes de restaurar um banco de dados do Exchange 2007 em um grupo de armazenamento de recuperação, você deve criar um grupo de armazenamento de recuperação e um banco de dados de caixa de correio com o mesmo nome.

Por exemplo, se desejar restaurar MailboxDatabase1 do primeiro grupo de armazenamento para um grupo de armazenamento de recuperação, é preciso criar um grupo de armazenamento de recuperação e adicionar o banco de dados "MailboxDatabase1" ao grupo de armazenamento de recuperação.

Observação: essa opção não se aplica ao Microsoft Exchange Server 2003

Desmontar o banco de dados antes de restaurar e montar o banco de dados após a restauração

Em geral, antes de uma restauração, o Microsoft Exchange executará algumas verificações para garantir:

- Que o banco de dados a ser restaurado esteja no status "Desmontado".
- Que o banco de dados não seja restaurado de forma inesperada.

  Para proteger um banco de dados de produção do Microsoft Exchange contra restauração inesperada, o switch é adicionado para permitir que o banco de dados seja substituído durante o processo de restauração. O Microsoft Exchange não fará a restauração de um banco de dados se essa opção não estiver definida.

Para o CA ARCserve D2D, estas duas opções são controladas por esta opção "Desmontar o banco de dados antes de restaurar e montá-lo após restauração". Com esta opção, o CA ARCserve D2D permite iniciar o processo de restauração automaticamente sem nenhuma operação manual. (É possível também especificar a desmontagem/montagem do banco de dados manualmente).

- Se marcada, especifica que o processo de recuperação desmontará automaticamente o banco de dados do Exchange antes do processo de restauração e, em seguida, montará o banco de dados após a conclusão do processo de restauração. Além disso, se estiver marcada, esta opção também permite que o banco de dados do Exchange seja substituído durante a restauração.
- Se estiver desmarcada, essa opção especifica que o processo de recuperação não desmontará automaticamente o banco de dados do Exchange antes da recuperação e o montará após a recuperação.

  O administrador do Exchange deve fazer algumas operações manuais como desmontar o banco de dados do Exchange, definir o sinalizador Permitir substituição no banco de dados e montar o banco de dados do Exchange. (O procedimento de recuperação é realizado pelo Exchange durante a montagem do banco de dados).

  Além disso, se não estiver marcada, esta opção não permite que o banco de dados do Exchange seja substituído durante a restauração.

Restaurar no banco de dados para recuperação (Exchange 2010)

Restaura o banco de dados em um banco de dados de recuperação. Um banco de dados de recuperação é um banco de dados que pode ser usado para fins de recuperação. É possível restaurar um banco de dados da caixa de correio do Microsoft Exchange a partir de um backup em um banco de dados de recuperação, bem como recuperar e extrair seus dados, sem afetar o banco de dados de produção que estiver sendo acessado por usuários finais.

Antes de restaurar um banco de dados do Exchange 2010 em um banco de dados de recuperação, é necessário primeiramente criar um banco de dados de recuperação.

Observação: essa opção não se aplica ao Microsoft Exchange Server 2003 e 2007.

9. Clique em Avançar para abrir a caixa de diálogo Resumo da restauração.
10. Examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.
    - Se as informações de resumo não estiverem corretas, clique em Anterior e volte à caixa de diálogo em questão para alterar a configuração incorreta.
    - Se as informações de resumo estiverem corretas, clique em Concluir para iniciar o processo de restauração.

Restaurar dados do SQL Server

Você pode executar restaurações em nível de aplicativo dos dados do Microsoft SQL Server com o seguinte:

- Microsoft SQL Server 2005 Express, Standard, Workgroup e Enterprise
- Microsoft SQL Server 2008, SQL Server 2008 R2 Express, Web, Standard, Workgroup e Enterprise

Observação: antes de começar, leia os pré-requisitos contidos no tópico Restaurações em nível de aplicativo (na página 105).

Importante: A restauração granular do Microsoft SQL Server não funciona no console do CA ARCserve Central Host-Based VM Backup. Para restaurar os dados do Microsoft SQL Server, instale o CA ARCserve D2D na máquina virtual convidada.

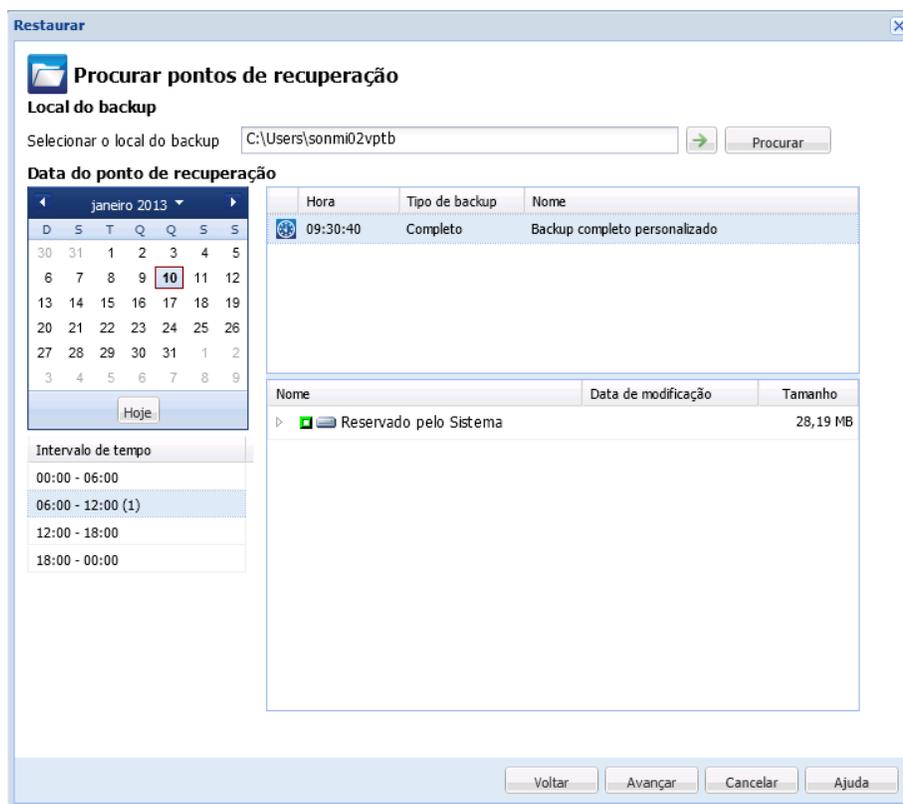
Siga estas etapas:

1. Verifique se o CA ARCserve D2D está instalado no sistema operacional convidado.
2. Efetue logon no sistema operacional convidado da máquina virtual em que deseja fazer a restauração de dados do SQL Server.
3. Inicie o CA ARCserve D2D e, em seguida, clique em Restaurar no painel de navegação do CA ARCserve D2D para abrir a caixa de diálogo Restaurar.

4. Clique em Procurar pontos de recuperação para abrir a caixa de diálogo Procurar pontos de recuperação.

5. No campo Selecionar local de backup na caixa de diálogo Procurar pontos de recuperação, especifique o caminho para a sessão de backup na máquina virtual do Host-Based VM Backup da qual deseja restaurar os dados do SQL Server. O caminho a seguir é um exemplo do caminho para a sessão de backup na máquina virtual do Host-Based VM Backup:

   ```
   https://<nome do servidor>/<nome do compartilhamento> /vm@<nome do host ou
   endereço IP do sistema ESX Server>
   ```

6. Selecione o ponto de recuperação (data e hora) e, em seguida, selecione o banco de dados do Microsoft SQL Server a ser restaurado.

7. Clique em Avançar para abrir a caixa de diálogo Opções de restauração.

   Selecione o destino da restauração. As opções disponíveis permitem restaurar no local original do backup, restaurar somente o arquivo de despejo ou restaurar em um local alternativo.

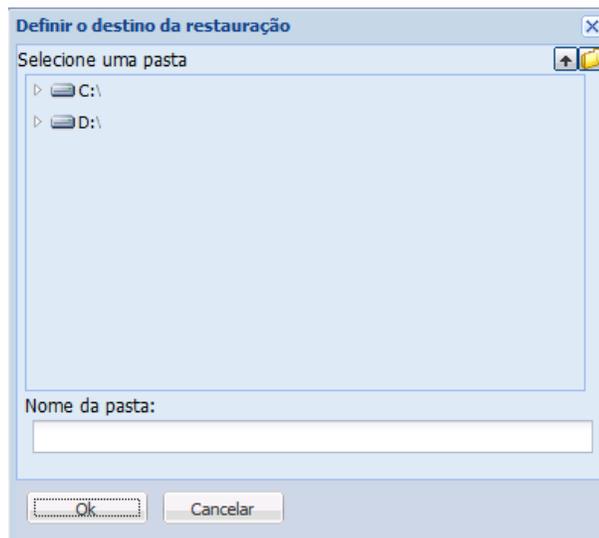
   Restaurar no local original

   Restaura no local original a partir do qual a imagem de backup foi capturada.

   Apenas arquivo de despejo

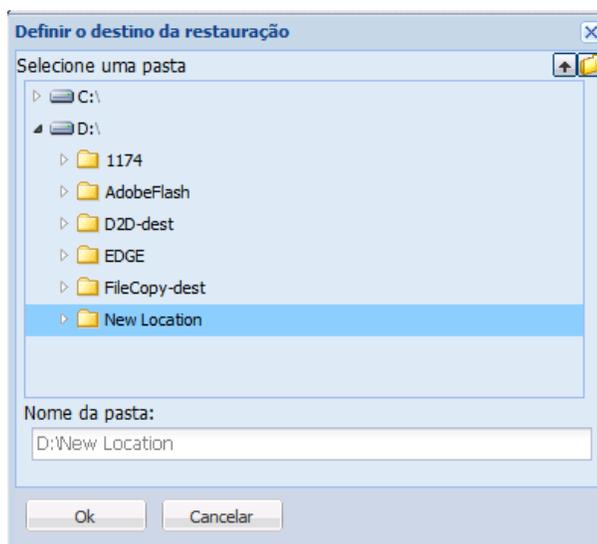
   Restaura apenas os arquivos de despejo.

   Os arquivos de despejo são criados quando um aplicativo falha e contém informações adicionais (com carimbo de data e hora) que podem ser usadas para solucionar a causa do problema.

   Ao selecionar essa opção, você pode especificar ou procurar o local da pasta em que o arquivo de despejo será restaurado.

   Restaurar em um local alternativo

   Restaura em um local diferente (que não seja o local original).

Nome da sessão	Nome do banco de dados	Nome do novo banco de dados	Local do arquivo alternativo
ARCSERVE_APP	ARCAppDB	ARCAppDB	Procurar

Como os backups podem ser copiados em locais de rede, eles podem ser usados por várias instâncias do SQL Server. É possível executar (simultaneamente) várias restaurações de banco de dados em nível de instância. Nesta listagem, você pode selecionar a instância do banco de dados e especificar um novo nome de banco de dados e o local alternativo em que restaurá-lo. Além disso, você também pode ir até o local alternativo em que o banco de dados será restaurado.

8. Clique em Avançar para abrir a caixa de diálogo Resumo da restauração.

9. Examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.

   - Se as informações de resumo não estiverem corretas, clique em Anterior e volte à caixa de diálogo em questão para alterar a configuração incorreta.

   - Se as informações de resumo estiverem corretas, clique em Concluir para iniciar o processo de restauração.

Capítulo 5: Solução de Problemas do CA ARCserve Central Host-Based VM Backup

Esta seção fornece informações sobre solução de problemas para ajudá-lo a identificar e resolver problemas que possam ocorrer durante o uso do <egvis>.

Esta seção contém os seguintes tópicos:

Mensagens do tipo "Não é possível estabelecer conexão com o servidor especificado" são exibidas ao tentar adicionar nós

Válido em plataformas Windows.

Sintoma:

A mensagem a seguir é exibida quando se tenta adicionar ou estabelecer conexão com os nós da tela Nó.

```
Não é possível se conectar ao servidor especificado.
```

Solução:

Se a mensagem acima for exibida ao tentar adicionar nós a partir da tela Nó, as seguintes ações corretivas ajudam a resolver o problema:

- Verifique se o serviço do Windows Server está em execução na máquina virtual de origem (nó) e no servidor do CA ARCserve Central Host-Based VM Backup.
- Verifique se uma exceção do Windows Firewall foi aplicada ao serviço de compartilhamento de arquivo e impressora do Windows na máquina virtual de origem (nó) e no servidor do CA ARCserve Central Host-Based VM Backup.
- Verifique se uma exceção do Windows Firewall foi aplicada ao serviço Netlogon do Windows apenas se o nó não for integrante de um domínio. Execute esta tarefa na máquina virtual de origem (nó) e no servidor do CA ARCserve Central Host-Based VM Backup.
- Verifique se o valor aplicado ao modelo de compartilhamento e segurança para contas locais é Clássico. Para aplicar o valor Clássico proceda da seguinte maneira:

  Observação: execute as etapas a seguir na máquina virtual de origem (nó) e no servidor do CA ARCserve Central Host-Based VM Backup.

  1. Efetue logon no servidor do CA ARCserve Central Host-Based VM Backup e abra o Painel de controle.
  2. No Painel de controle, abra Administrative Tools.
  3. Clique duas vezes em Diretiva de segurança local.

     A janela Diretiva de segurança local é exibida.

4. Nesta janela, expanda Diretivas locais e expanda Opções de segurança.

   As diretivas de segurança são exibidas.

5. Clique com o botão direito do mouse em Network access: Sharing and security model for local accounts e clique em Propriedades no menu pop-up.

   A caixa de diálogo Network access: Sharing and security model for local accounts properties é exibida.

6. Clique em Configuração de segurança local.

   Na lista suspensa, selecione Clássico - os usuários locais são autenticados como eles mesmos.

   Clique em OK.

- Verifique se o valor aplicado às Diretivas locais para o nível de autenticação do LAN Manager é definido para enviar LM & NTLMv2 - usar a segurança da sessão NTLMv2, se negociado. Para aplicar o valor, proceda da seguinte maneira:

  1. Efetue logon no servidor do CA ARCserve Central Host-Based VM Backup e abra o prompt de comando.

     Execute o seguinte comando

     ```
     secpol.msc
     ```

     A caixa de diálogo Configurações locais de segurança é exibida.

  2. Selecione as diretivas locais e clique em opções de segurança.

     Pesquise a segurança de rede: nível de autenticação do LAN Manager.

     Clique duas vezes na opção.

     A caixa de diálogo Propriedades é aberta

  3. Selecione a opção a seguir e clique em OK.

     ```
     enviar LM & NTLMv2 - usar a segurança da sessão NTLMv2, se negociado
     ```

  4. No prompt de comando, execute o seguinte:

     ```
     gpupdate
     ```

  O valor é aplicado.

Páginas da web em branco são exibidas ou ocorrem erros no Javascript

Válido para os sistemas operacionais Windows Server 2008 e Windows Server 2003.

Sintoma:

Ao abrir os sites da web do CA ARCserve Central Applications usando o Internet Explorer, páginas da web em branco são exibidas ou ocorrem erros no Javascript. O problema ocorre ao abrir o Internet Explorer em sistemas operacionais Windows Server 2008 e Windows Server 2003.

Esse problema ocorre nas seguintes condições:

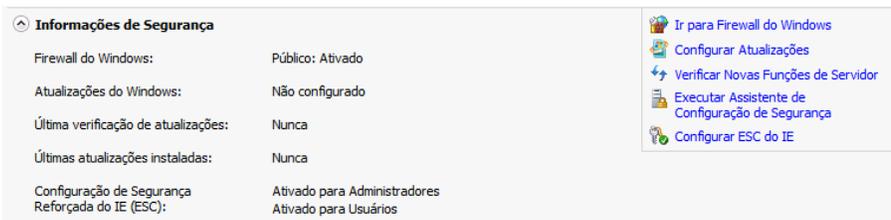
- Você está usando o Internet Explorer 8 ou Internet Explorer 9 para exibir o aplicativo e o navegador não reconhece o URL como um site confiável.
- Você está usando o Internet Explorer 9 para exibir o aplicativo e o protocolo de comunicação em uso é HTTPS.

Solução:

Para corrigir este problema, desative a opção Segurança aprimorada do Internet Explorer nos computadores usados para exibir o aplicativo.

Para desativar esta opção em sistemas Windows Server 2008, faça o seguinte:

1. Faça logon no computador com Windows Server 2008 que você usa para exibir os relatórios usando a conta de administrador ou uma conta que tenha privilégios administrativos.
2. Clique com o botão direito do mouse em Computador na área de trabalho e clique em Gerenciar para abrir a janela Gerenciador do servidor.
3. Na janela Gerenciador do servidor, clique em Gerenciador do servidor (nome do servidor).

   Na seção Server Summary, abra Security Information e clique em Configure IE ESC, conforme ilustrado abaixo:

   A caixa de diálogo Enhanced Security Configuration do Internet Explorer é aberta.

4. Neste caixa de diálogo, faça o seguinte:
   - Administrators--Click Desativado
   - Usuários--Clique em Desativar.

   Clique em OK.

A caixa de diálogo Internet Explorer Enhanced Security Configuration é fechada e segurança reforçada do Internet Explorer é desativada.

Para desativar esta opção em sistemas Windows Server 2003, faça o seguinte:

1. Faça logon no computador com Windows Server 2003 que você usa para exibir os relatórios usando a conta de administrador ou uma conta que tenha privilégios administrativos.
2. Abra o Painel de Controle do Windows e, em seguida, abra Add or Remove Programs.
3. Na caixa de diálogo Add or Remove Programs, clique na opção Add/Remove Windows Components para acessar a tela Windows Components Wizard.

   Desmarque a caixa de seleção próxima a Configuração de segurança aprimorada do Internet Explorer.

   Clique em Avançar.

   Siga as instruções na tela para concluir a instalação e clique em Concluir.

A opção Internet Explorer Enhanced Security é desativada.

As páginas da web não são carregadas corretamente ao efetuar logon nos nós do CA ARCserve D2D

Válido em plataformas Windows.

Sintoma:

As páginas da web em janelas do navegador não são carregadas corretamente, exibem mensagens de erro, ou ambos, ao efetuar logon em nós do CA ARCserve D2D na tela Nós.

Solução:

Esse comportamento afeta principalmente os navegadores Internet Explorer. As páginas da web podem não ser carregadas corretamente quando scripts ativos, controles ActiveX ou programas Java estiverem desativados no computador ou bloqueados na rede.

É possível corrigir o problema com a atualização da janela do navegador. No entanto, se a atualização do navegador não corrigir o problema, faça o seguinte:

1. Abra o Internet Explorer.

   No menu Ferramentas, clique em Opções da Internet.

   A caixa de diálogo Opções da Internet é aberta.

2. Clique na guia Segurança.

   As opções de segurança são exibidas:

3. Clique em Zona da Internet.

   As opções de zona da Internet são exibidas.

4. Clique em Nível personalizado.

   A caixa de diálogo Security Settings - Internet Zone é aberta.

5. Rolar para a categoria Script.

   Localize o Script ativo.

   Clique na opção Ativar ou Solicitar.

6. Clique em OK na caixa de diálogo Security Settings - Internet Zone.

   A caixa de diálogo Security Settings - Internet Zone é fechada.

7. Clique em OK na caixa de diálogo Internet Options.

   Esta caixa de diálogo é fechada e a opção Script ativo é aplicada.

Observação: se esta solução não corrigir o problema, consulte o administrador do sistema para verificar se os outros programas, como programas antivírus ou de firewall, não estão bloqueando os scripts ativos, os controles ActiveX ou os programas do Java.

Resolução de problemas do carregamento da página

Válido em plataformas Windows.

Sintoma:

As seguintes mensagens de erro podem ser exibidas em janelas de navegador ao efetuar logon em nós do CA ARCserve Central Applications, CA ARCserve D2D e servidores de monitoramento.

Mensagem 1:

```
Os erros nesta página podem fazer com que ela funcione incorretamente.
```

Mensagem 2:

```
!
```

Solução:

As páginas da web podem não ser carregadas corretamente por vários motivos. A tabela a seguir descreve os motivos comuns e as respectivas ações corretivas:

Razão	Ação corretiva
Há problemas com o código fonte HTML subjacente.	Atualize a página da web e tente novamente.
Sua rede bloqueia o Script ativo, ActiveX, ou os programas Java.	Permita que seu navegador use Script ativo, ActiveX ou programas Java.
Seu aplicativo antivírus está configurado para examinar arquivos temporários da Internet e programas cujo download foi concluído.	Filtre o aplicativo antivírus para permitir arquivos relacionados à Internet associados a páginas da web do CA ARCserve Central Applications.
O mecanismo de script instalado em seu computador está corrompido ou desatualizado.	Atualize o mecanismo de script.
A placa de vídeo instaladas no computador estão corrompidas ou desatualizadas.	Atualize-as.
O componente DirectX instalado em seu computador está corrompido ou desatualizado.	Atualize-o.

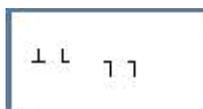
Caracteres sem sentido são exibidos no navegador do Windows ao acessar o CA ARCserve Central Applications

Válido em todos os sistemas operacionais Windows. Todos os navegadores afetados.

Sintoma:

Ao efetua logon no CA ARCserve Central Applications, caracteres sem sentido aparecem na área de conteúdo da janela do navegador.

Solução:

Este problema ocorre ao instalar o CA ARCserve Central Applications usando a comunicação HTTPS e ao tentar acessar o CA ARCserve Central Applications usando a comunicação HTTP. O componente subjacente dos serviços web do CA ARCserve Central Applications não oferece suporte ao recurso para converter URLs HTTP para URLs HTTPS. Como resultado, os caracteres sem sentido aparecem na janela do navegador. Por exemplo:

Para corrigir esse problema, acesse o CA ARCserve Central Applications usando o HTTPS ao instalar ou configurar aplicativos para se comunicar usando o HTTPS.

Erros de acesso negado ao atualizar os nós

Válido em todos os sistemas operacionais Windows com suporte ao UAC (User Account Control - Controle de Conta de Usuário).

Observação: Windows Vista ou versões posteriores.

Sintoma 1:

Ao fornecer uma conta de usuário do Windows que não é uma conta de administrador interno ou de usuário de domínio, mas que é integrante do grupo de administradores, as seguintes mensagens são exibidas ao se aplicar a senha na caixa de diálogo Credenciais do nó da caixa de diálogo Importar máquinas virtuais do vCenter/ESX:

`É necessário ter privilégio de administrador.`

O resultado disso é que você não pode aplicar as credenciais do nó.

Sintoma 2:

Quando você importa os nós, mas não fornece as credenciais durante a operação de importação, a seguinte mensagem é exibida durante a tentativa de execução da operação Atualizar nó, usando uma conta de usuário do Windows que não é uma conta de administrador interno ou de usuário de domínio, mas que é integrante do grupo de administradores:

```
Acesso negado. Verifique se o usuário tem privilégio de administrador e se o acesso
ao Registro remoto não está bloqueado por uma diretiva de segurança local da máquina
adicionada.
```

O resultado disso é que você não pode atualizar o nó.

Solução:

Você pode esperar este comportamento quando o UAC está ativado em computadores executando o sistema operacional Windows com suporte ao UAC. O UAC é um recurso do Windows que permite apenas que a conta de administrador efetue logon no computador a partir de um local remoto.

Use um dos seguintes métodos para resolver esse problema:

- Forneça as credenciais internas ou do administrador de domínio.
- Desativar o UAC:
    1. Efetue logon no nó usando a conta de administrador.
    2. Abra o Painel de Controle do Windows.
    3. Abra Contas de Usuário.
    4. Na tela Fazer alterações na conta de usuário, clique em Alterar configurações de Controle de Conta de Usuário e, em seguida, execute um dos seguintes procedimentos:
        - **Windows Vista e Windows Server 2008:** na tela Fazer alterações na conta de usuário, clique em Ativar ou desativar o Controle de Conta de Usuário. Em seguida, na tela Ativar o Controle de Conta de Usuário (UAC) para tornar o computador mais seguro, desmarque a caixa de seleção ao lado de Utilizar o Controle de Conta de Usuário (UAC) para ajudar a proteger o computador e clique em OK.

          Reinicie seu computador para aplicar as alterações ao UAC.
        - **Windows Server 2008 r2 e Windows 7:** na tela Definir quando deverá ser notificado sobre alterações no computador, mova o controle deslizante de Sempre notificar para Nunca notificar. Clique em OK e feche o Painel de controle do Windows.

          Reinicie seu computador para aplicar as alterações ao UAC.

Erro de certificado é exibido ao efetuar logon no aplicativo

Válido em plataformas Windows.

Sintoma:

A seguinte mensagem é exibida na janela do navegador ao efetuar logon no aplicativo:

- Internet Explorer:

  `Há um problema com o certificado de segurança do site.`

- Firefox:

  `Esta conexão não é confiável.`

- Chrome:

  `O certificado de segurança do site não é confiável.`

Se você especificar uma opção que permita continuar com o site, será possível efetuar logon no aplicativo com êxito. No entanto, você encontrará este comportamento toda vez que efetuar logon no aplicativo.

Solução:

Este comportamento ocorre ao especificar o uso de HTTPS como o protocolo de comunicação. Para corrigir esse problema temporariamente, clique no link na janela do navegador que permite continuar com o site. No entanto, da próxima vez que você efetuar logon no aplicativo, você verá esta mensagem novamente.

O protocolo de comunicação HTTPS fornece um nível maior de segurança do que o protocolo de comunicação HTTP. Caso deseje continuar a se comunicar usando o protocolo de comunicação HTTPS, é possível adquirir um certificado de segurança do VeriSign e instalar o certificado no servidor do aplicativo. Como opção, é possível alterar o protocolo de comunicação usado pelo aplicativo para HTTP. Para alterar o protocolo de comunicação para HTTP, faça o seguinte:

1. Faça logon no servidor onde instalou o aplicativo.
2. Vá para o seguinte diretório:

   `C:\Arquivos de programas\CA\ARCserve Central Applications\BIN`

3. Execute o seguinte arquivo em lotes:

   `ChangeToHttp.bat`

4. após executar este arquivo, abra o Gerenciador de servidores do Windows.

   Reinicie o seguinte serviço:

   `Serviço do CA ARCserve Central Applications`

Os backups falham com erros de criação de instantâneo

Válido em plataformas Windows.

Ao enviar backups do VMware com base em máquinas virtuais, os seguintes sintomas ocorrem:

Sintoma 1

As tarefas de backup falham e a mensagem a seguir é exibida no Log de atividades:

```
Falha ao criar instantâneo. Erro de relatório do ESX/vCenter. Ocorreu um erro geral de sistema. Erro de protocolo de VMX.
```

Solução 1

Esse erro é um problema do VMware. Para corrigir o problema, desinstale e reinstale o VMware Tools no sistema operacional convidado e envie a tarefa novamente.

Sintoma 2

As tarefas de backup falham e a mensagem a seguir é exibida no Log de atividades:

```
Não foi possível obter instantâneo da máquina virtual. O ESX Server/vCenter Server relatou o seguinte erro: Não é possível criar um instantâneo fechado, pois a operação de criação de instantâneo excedeu o limite de tempo para desativar a E/S na máquina virtual congelada.
```

Solução 2

Este erro ocorre quando o VSS encontra erros durante a criação de instantâneos. O VSS pode encontrar erros nas seguintes condições:

Um gravador VSS está em um estado instável.

Para determinar a origem e corrigir esse comportamento, execute as seguintes ações corretivas:

1. Execute o comando "vssadmin list writers" na linha de comando do sistema operacional convidado da máquina virtual.
2. Verifique se todos os gravadores VSS se encontram em um estado íntegro.
3. Para gravadores que estão nos seguintes estados, entre em contato com a Microsoft ou com o fornecedor do gravador para obter informações sobre como corrigir os erros.

   ```
   estado=Falhou
   Último erro = Sem erro
   ```

   Observação: reiniciar os gravadores geralmente resolve o problema.

O VSS encontrou erros ao criar instantâneos.

Para determinar a origem e corrigir esse comportamento, execute as seguintes ações corretivas:

1. Examine o log de eventos do Windows no sistema operacional convidado. Verifique se existem erros relacionados aos componentes VSS sobre a hora em que o backup foi iniciado.
2. Quando o VSS relata erros devido ao espaço em disco insuficiente, libere espaço em disco no volume associado ao erro.
3. Quando o VSS ou o driver do Windows Volsnap gera erros de tempo esgotado, os aplicativos em execução na máquina virtual estão em um estado altamente ativo. O estado altamente ativo evita que o VSS crie instantâneos de maneira consistente. Para solucionar essa condição, agendar backups quando os aplicativos realizam menos operações de entrada e saída para o volume.
4. Quando o Log de eventos do Windows indica que o driver VolSnap encontrou erros, consulte o artigo do Integridade do driver de instantâneo de volume na Biblioteca Technet da Microsoft para obter informações sobre como corrigir erros do driver VolSnap.

Falha nas operações da VM com erros desconhecidos

Válido em sistemas operacionais Windows.

Sintoma:

Falha nas tarefas de recuperação da VM. É possível enviar a tarefa Recuperar VM, no entanto, a seguinte mensagem é exibida no log de atividades:

```
Falha ao recuperar os discos virtuais.
```

Além disso, o VDDK relata a seguinte mensagem de erro:

```
Erro desconhecido.
```

Solução 1:

Para resolver esse problema, considere as seguintes soluções:

- Ocorre falha nas tarefas Recuperar VM quando não há espaço em disco suficiente no armazenamento de dados original. O VDDK retorna a mensagem, pois a API do VDDK (no momento) não oferece suporte ao recurso para detectar a quantidade de espaço livre em disco no armazenamento de dados original. (O armazenamento de dados é o local em que se especifica a recuperação da máquina virtual.) Para corrigir esse problema, libere a quantidade de espaço em disco no armazenamento de dados original necessária para que a operação seja concluída e, em seguida, reenvie a tarefa.
- Interferências e excesso de tráfego na rede podem causar falha nas tarefas Recuperar VM. Para corrigir o problema, certifique-se de que o sistema do servidor de proxy e o do ESX Server ou vCenter Server possam se comunicar pela rede e, em seguida, reenvie a tarefa.
- Várias conexões simultâneas que consistem em tarefas de backup ou de recuperação via VM para o sistema ESX Server ou vCenter Server, que inclui as conexões SDK do vSphere por meio do cliente vSphere para VMware, podem provocar a falha das tarefas. Para corrigir este problema, feche todas as conexões desnecessárias e, em seguida, reenvie a tarefa. Para obter informações sobre a quantidade máxima de conexões simultâneas permitidas, consulte o tópico Não é possível abrir arquivo VMDK (na página 144).
- Examine as seções de tarefas e eventos do log do cliente VMware vSphere para descobrir erros internos de uma máquina virtual específica. Corrija os erros internos e, em seguida, reenvie a tarefa.

  Exemplo: outro aplicativo ou operação está usando o arquivo VMDK. Para corrigir o problema, libere o arquivo e reenvie a tarefa.

Solução 2:

Este problema poderá ocorrer nas seguintes condições:

- O VDDK não pôde processar um instantâneo corretamente.
- O VDDK não pôde excluir o instantâneo manualmente ou ele é interno para a máquina virtual.

Para corrigir esse problema, envie a tarefa novamente. Caso a tarefa falhe novamente, exclua a máquina virtual recuperada e envie a tarefa novamente.

Não é possível montar discos com operações de backup e recuperação usando o modo de transporte hotadd

Válido em plataformas Windows.

Sintoma:

As tarefas de backup e recuperação que usam o modo de transporte hotadd não podem montar discos no sistema proxy.

Solução:

Para resolver esse problema, faça o seguinte:

1. Abra o VMware vSphere Client.

   Efetue logon no sistema do ESX Server ou vCenter Server usando credenciais administrativas.

2. Selecione a máquina virtual do proxy e edite suas configurações.
3. Remova os discos hotadd conectados à máquina virtual de origem ou à máquina virtual proxy.
4. Envie a tarefa novamente.

As operações de recuperação falham ao recuperar dados usando o modo de transporte hotadd ou SAN

Válido em plataformas Windows.

Sintoma:

As operações de recuperação falham ao recuperar dados usando o modo de transporte hotadd ou SAN. A seguinte mensagem é exibida no log de atividades:

`Ocorreu um erro desconhecido. Entre em contato com o suporte técnico.`

Solução:

As operações de recuperação falham ao usar o modo de transporte hotadd (na página 195) ou SAN (na página 195) quando as configurações de disco não estiverem definidas corretamente.

Para configurar o disco, execute as seguintes etapas:

1. Efetue logon no sistema proxy de backup usando uma conta com privilégios administrativos.
2. Abra a linha de comando do Windows.

3. Na linha de comando, digite o seguinte comando:

   `diskpart`

   Pressione Enter.

4. Digite SAN e, em seguida, pressione Enter.

   A diretiva atual da SAN é exibida.

5. Digite o seguinte comando:

   `SAN POLICY = OnlineAll`

   Pressione Enter.

   A diretiva da SAN está configurada para não montar automaticamente volumes hospedados pela SAN.

6. Para limpar o atributo de somente leitura do disco específico da SAN, selecione o disco a partir da lista de discos e digite o seguinte comando:

   `attribute disk clear readonly`

   Pressione Enter.

7. Digite exit e, em seguida, pressione Enter.

O disco está configurado e é possível enviar a tarefa novamente.

Se a tarefa falhar novamente, monte os discos hotadd manualmente usando o gerenciamento de discos no sistema proxy.

Para montar os discos manualmente, faça o seguinte:

1. Efetue logon no sistema proxy de backup usando uma conta com privilégios administrativos.

2. Abra o Painel de Controle do Windows e clique duas vezes em Ferramentas Administrativas.

   A janela Ferramentas Administrativas é exibida.

3. Na lista Favoritos, clique duas vezes em Gerenciamento do Computador.

   O Gerenciamento do computador é exibido.

4. Expanda Armazenamento e clique em Gerenciamento de Disco.

   Os discos são exibidos.

5. Clique com o botão direito no disco que deseja montar e clique em Online.

O disco está montado e é possível enviar a tarefa novamente.

Ocorrem erros Sistema operacional não encontrado

Válido em plataformas Windows.

Sintoma 1

A mensagem a seguir é exibida quando você tenta iniciar o sistema operacional convidado em uma máquina virtual após recuperar a máquina virtual usando a opção Restaurar em um local diferente:

```
Sistema operacional não encontrado.
```

Solução 1

Esse comportamento pode ocorrer em máquinas virtuais que contenham dispositivos SCSI e IDE. Se esse problema ocorrer, examine a maneira como os discos estão configurados na máquina virtual e verifique se a sequência de inicialização da máquina virtual recuperada é igual à da máquina virtual de origem. Se a sequência de inicialização for diferente, será preciso atualizar o BIOS na máquina virtual recuperada para corresponder ao da origem.

Observação: o primeiro disco IDE deve usar (0:1).

Sintoma 2

a mensagem a seguir é exibida quando você tenta iniciar o sistema operacional convidado em uma máquina virtual após recuperar a máquina virtual:

```
Sistema operacional não encontrado.
```

Solução 2

Se esse problema ocorrer, examine a maneira como os discos estão configurados na máquina virtual e verifique se a sequência de inicialização da máquina virtual de réplica é igual à da máquina virtual de origem.

As alterações do endereço MAC não são retidas após a recuperação da VM

Válido em plataformas Windows.

Sintoma:

Os endereços MAC de máquinas virtuais não são mantidos após a recuperação de máquinas virtuais.

Solução:

Os endereços MAC não são mantidos durante a recuperação, para evitar duplicatas. Para manter as informações de endereços MAC, defina a seguinte chave do Registro no servidor proxy:

```
Local: SOFTWARE\CA\CA ARCSERVE D2D
Nome da chave: RetainMACForVDDK
Tipo de valor: String
Valor da chave: 1
```

Em máquinas virtuais com duas placas NIC, defina a chave do Registro RetainMACForVDDK se desejar definir uma delas como manual. Caso contrário, todas as placas serão definidas como Automática após a recuperação.

Falha de serviço web do CA ARCserve D2D em nós do CA ARCserve D2D

Válido em plataformas Windows.

Sintoma:

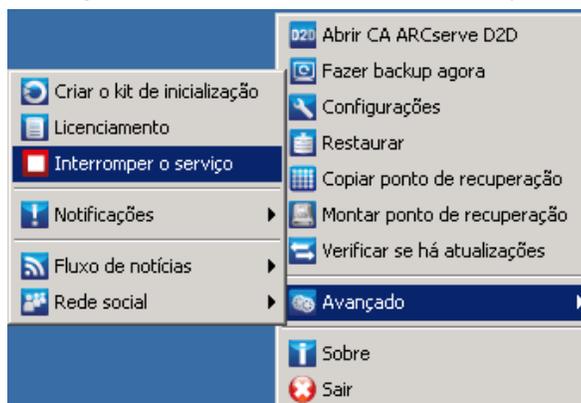
O serviço web em execução em nós do CA ARCserve D2D é iniciado e falha ou não pode ser iniciado.

Solução:

Esse problema ocorre quando a porta usada pelo serviço web do CA ARCserve D2D é a mesma que a porta usada pelo serviço web do VMware vCenter (Tomcat).

A porta usada pelo CA ARCserve D2D pode entrar em conflito com a porta padrão usada pelo Tomcat. Esse conflito gera falha no Tomcat quando o CA ARCserve D2D é iniciado antes dele. Para corrigir este problema, pode-se alterar a porta padrão do Tomcat, como segue:

1. Acesse o monitor do CA ARCserve D2D, clique na opção Avançado e selecione Interromper o serviço.

   O serviço web do CA ARCserve D2D é interrompido.

2. Acesse o arquivo server.xml para editar/configurar o comportamento do Tomcat.

   O arquivo server.xml está localizado na seguinte estrutura de pastas:

   `C:\Arquivos de programas\CA\ARCserve Central Applications\TOMCAT\conf`

3. Localize a marca <Server> no arquivo server.xml.

4. Edite a marca <Server>, como segue:

   De:

   <Server>

   Para:

   <Server port="8015" shutdown="SHUTDOWN">

5. Salve e feche o arquivo server.xml.

   O comando para desligar o Tomcat agora foi configurado de forma que ele seja recebido pelo servidor na porta especificada (8015).

6. Acesse o monitor do CA ARCserve D2D, clique na opção Avançado e selecione Iniciar o serviço.

   O serviço web do CA ARCserve D2D é iniciado.

O CA ARCserve Central Host-Based VM Backup não pode se comunicar com o serviço web do CA ARCserve D2D em nós remotos

Válido em sistemas operacionais Windows.

Sintoma:

O CA ARCserve Central Host-Based VM Backup não pode se comunicar com o serviço web do CA ARCserve D2D em nós remotos.

Solução:

A tabela a seguir descreve os motivos pelos quais o CA ARCserve Central Host-Based VM Backup não pode se comunicar com o serviço web do CA ARCserve D2D em nós remotos e a ação corretiva correspondente:

Causa	Ação corretiva
A rede não está disponível ou não está estável ao aplicar diretivas.	Verifique se a rede está disponível e estável e tente novamente.
O computador do CA ARCserve D2D não pôde lidar com a carga quando o aplicativo tentou comunicar-se com o nó.	Verifique se a CPU no nó remoto do CA ARCserve D2D está em um estado normal e tente novamente.
O serviço do CA ARCserve D2D no nó remoto não estava em execução ao aplicar as diretivas.	Verifique se o nó remoto do CA ARCserve D2D está em execução e tente novamente.
O serviço do CA ARCserve D2D não está se comunicando adequadamente.	Reinicie este serviço do CA ARCserve D2D no nó remoto e tente novamente.

O serviço web do CA ARCserve D2Dé executado lentamente

Válido em sistemas operacionais Windows.

Sintoma 1:

O serviço web do CA ARCserve D2D em sistemas do CA ARCserve D2D é executado lentamente. É possível detectar outros sintomas, tais como:

- O serviço web do CA ARCserve D2D pára de responder ou ocupa 100% dos recursos da CPU.
- A comunicação dos nós do CA ARCserve D2D com o serviço web é insatisfatória ou não existe.

Solução 1:

Em diversas configurações de ambiente, é possível descobrir que o serviço web do CA ARCserve D2D ocupa muito tempo da CPU, ou a resposta é lenta. Por padrão, o Tomcat é configurado para alocar uma quantidade limitada de memória para os nós, que talvez não seja adequada para seu ambiente. Para verificar esse problema, revise os arquivos de log a seguir:

```
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stdout.*.log
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stder.*.log
<D2D_home>\TOMCAT\logs\catalina.*.log
<D2D_home>\TOMCAT\logs\localhost.*.log
```

Procure a seguinte mensagem:

```
java.lang.OutOfMemoryError
```

Para corrigir este problema, aumente a quantidade de memória alocada.

Para aumentar a memória, proceda da seguinte maneira:

1. Abra o Registry Editor e acesse a chave a seguir:
   - Sistemas operacionais x86:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun
     2.0\CASAD2DWebSvc\Parameters\Java
     ```

   - Sistemas operacionais x64:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun
     2.0\CASAD2DWebSvc\Parameters\Java
     ```

2. Siga um destes procedimentos:

   ■ Se a mensagem no arquivo de log for:

     ```
     java.lang.OutOfMemoryError: PermGen space
     ```

     Acrescente o seguinte valor de opções.

     ```
     -XX:PermSize=128M -XX:MaxPermSize=128M
     ```

     Observação: talvez seja necessário aumentar o valor de -XX:MaxPermSize de acordo com seu ambiente.

   ■ Se a mensagem no arquivo de log for:

     ```
     java.lang.OutOfMemoryError: Java heap space
     java.lang.OutOfMemoryError: GC overhead limit exceeded
     ```

     Aumente o valor de DWORD a seguir:

     ```
     JvmMx
     ```

3. Reinicie o serviço web do CA ARCserve D2D.

Sintoma 2

Os backups programados são ignorados e a execução é interrompida.

Solução 2

Ao configurar o valor MAX como 20 ou menos de 20 para backups simultâneos, faça o seguinte:

1. Aumente o valor de DWORD a seguir:

   ```
   JvmMx=256
   ```

   Observação: esse DWORD é mencionado na Solução 1.

2. Acrescente o seguinte valor de opções.

   ```
   -XX:MaxPermSize=128M
   ```

   Observação: esse DWORD é mencionado na Solução 1.

Ao configurar o valor MAX como mais de 20, mas menos que 50 para backups simultâneos, faça o seguinte:

1. Aumente o valor de DWORD a seguir:

   ```
   JvmMx=512
   ```

   Observação: esse DWORD é mencionado na Solução 1.

2. Acrescente o seguinte valor de opções.

   ```
   -XX:MaxPermSize=256M
   ```

   Observação: esse DWORD é mencionado na Solução 1.

Falhas do rastreamento do bloco alterado

Válido no Windows.

Sintoma:

Os backups da máquina virtual falham e o rastreamento do bloco alterado é ativado nas máquinas virtuais.

Solução:

A tabela a seguir descreve as condições ambientais que podem causar a falha dos backups da máquina virtual com rastreamento do bloco alterado ativado:

Condição	Solução
Instantâneos gerados pelo usuário estão presentes nas máquinas virtuais e o rastreamento do bloco alterado está desativado.	Ativar ou redefinir o rastreamento do bloco alterado para permitir que a tarefa de backup completa continue. **Observação**: a tarefa de backup completa continuará com os blocos de dados usados e não usados pelos arquivos VMDK.
A versão incorreta do hardware da VMware está instalada na máquina virtual.	Verifique se o hardware da VMware versão 7.0 ou posterior está instalado na máquina virtual.
A versão incorreta do ESX Server está instalada na máquina virtual.	Verifique se o ESX Server versão 4.0 ou posterior está instalado na máquina virtual.
O sistema ESX Server encontrou um encerramento abrupto. Encerramentos abruptos podem causar falhas de backup do rastreamento do bloco alterado.	O CA ARCserve Central Host-Based VM Backup ativa automaticamente o rastreamento do bloco alterado na máquina virtual.
O sistema ESX Server encontrou uma reinicialização (limpar) enquanto a máquina virtual estava ligada.	O CA ARCserve Central Host-Based VM Backup ativa automaticamente o rastreamento do bloco alterado na máquina virtual.
A máquina virtual foi movida usando o Storage vMotion.	O CA ARCserve Central Host-Based VM Backup ativa automaticamente o rastreamento do bloco alterado na máquina virtual.

Os backups falham devido à licença ESXi

Válido em plataformas Windows.

Sintoma:

Falha nas tarefas de backup completo, incremental e de verificação do CA ARCserve D2D. A seguinte mensagem é exibida no log de atividades do CA ARCserve D2D:

```
O servidor <server_name> da VM não tem uma licença paga do ESX
```

Solução:

Devido a uma limitação do VMware, as máquinas virtuais em execução em servidores ESXi com uma licença gratuita não podem ser copiadas para backup. Para proteger as VMs, aplique uma licença adquirida.

Os backups falham e o evento 1530 é registrado no log de eventos do sistema proxy de backup

Válido em plataformas Windows.

Sintoma:

As tarefas do CA ARCserve Central Host-Based VM Backup falham. O evento 1530 é registrado no Log de eventos do aplicativo no sistema proxy de backup.

Ambiente/etapas para reproduzir:

- O Microsoft SQL Server ou o Microsoft Exchange Server está instalado na máquina virtual.
- O usuário efetua logon ou já está conectado ao servidor proxy do CA ARCserve Central Host-Based VM Backup usando a conta de administrador ou uma conta membro do grupo de administradores.
- Após o início da tarefa de backup, o usuário efetua logoff do servidor proxy.
- A tarefa de backup falha. O evento 1530 é registrado no log de Eventos do aplicativo.

  ```
  Aviso... O serviço de perfil do usuário do Microsoft Windows 1530 Nenhum O Windows detectou que seu arquivo de registro ainda está sendo usado por outros aplicativos ou serviços. O arquivo será descarregado agora. Os aplicativos ou serviços que contêm seu arquivo de registro poderão não funcionar corretamente posteriormente.
  ```

Causa:

O Windows Server 2008 contém um Serviço de Perfil de Usuário que descarrega perfis de usuário quando usuários fazem logoff do computador. Como resultado, os objetos COM não podem ser criados, o que impede o Host-Based VM Backup chamar os módulos COM.

Solução:

Para impedir que as tarefas de backup falhem, execute as seguintes etapas:

Observação: para essa solução funcionar, todos os sintomas listados acima devem estar presentes.

1. Efetue o logon no servidor proxy do Host-Based VM Backup usando a conta de administrador ou uma conta membro do grupo de administradores.
2. Iniciar o Editor de Diretiva de Grupo Local digitando gpedit.msc na caixa de diálogo Executar.
3. No Editor de Diretiva de Grupo Local, expanda Configuração do sistema, Modelos administrativos, Sistemas e Perfis de usuário.
4. No diretório Perfis de usuário, clique duas vezes em **Não forçar o descarregamento do registro de usuário no logoff do usuário** para abrir a caixa de diálogo **Não forçar o descarregamento do registro de usuário no logoff do usuário**.
5. Na caixa de diálogo **Não forçar o descarregamento do registro de usuário no logoff do usuário**, clique em Ativado e em OK.

   Observação: o valor DisableForceUnload é adicionado ao Registro.
6. Reinicie o servidor do Host-Based VM Backup.

Os backups são concluídos usando o modo de transporte NBD quando o modo de transporte hotadd é especificado

Válido em plataformas Windows.

Sintoma:

Os backups de máquinas virtuais são concluídos usando o modo de transporte NBD (na página 195) quando o modo de transporte hotadd (na página 195) é especificado para o backup.

Solução:

O CA ARCserve Central Host-Based VM Backup permite fazer backup de máquinas virtuais que residam em sistemas ESX Server. Ao fazer backup de máquinas virtuais usando o modo de transporte hotadd, é possível conectar o máximo de 15 discos virtuais para cada controlador SCSI no servidor proxy da máquina virtual do CA ARCserve D2D. Ao enviar um backup que inclui mais de 15 discos virtuais e existe apenas um controlador SCSI no servidor proxy da máquina virtual do CA ARCserve D2D, esse único controlador SCSI não poderá acomodar todas as máquinas virtuais. Como resultado, o CA ARCserve Central Host-Based VM Backup faz o backup dos dados no modo de transporte NBD.

Para evitar que isso ocorra, verifique se há uma quantidade suficiente de controladores SCSI no servidor proxy da máquina virtual do CA ARCserve D2D que possa acomodar todas as máquinas virtuais na tarefa de backup.

A tarefa de backup incremental é processada como tarefas de backup de verificação

Válido no Windows.

Sintoma:

Ao enviar ou programar tarefas de backup incrementais que são processadas usando o modo de transporte Hotadd, o seguinte comportamento ocorre:

- As tarefas incrementais são convertidas para tarefas de backup de verificação. A entrada do Log de atividades para a tarefa indica que a tarefa de backup incremental foi convertida em uma tarefa de backup de verificação.
- O Snapshot Manager no VI Client, cuja máquina virtual foi feito backup, contém um instantâneo auxiliar consolidado.
- A caixa de diálogo Editar configurações no VI Client da máquina virtual afetada indica que não há discos anexados incorretamente ao sistema proxy de backup. As URLs do VMDK associadas com os discos incorretos não são as mesmas URLs do VMDK associadas com o sistema de proxy de backup.

Solução:

Para corrigir esse comportamento, remova os arquivos VMDK incorretos (discos) do sistema proxy de backup usando as orientações descritas no artigo de base de conhecimento VMware 1003302. Além disso, o VMware recomenda que o espaço livre de armazenamento de dados seja duas vezes o tamanho cumulativo de arquivos da máquina virtual.

Falha nas tarefas de backup, pois os blocos não podem ser identificados

Válido no Windows.

Sintoma:

As tarefas de backup de uma máquina virtual específica apresentam falhas, e a mensagem a seguir é exibida no log de atividades:

```
O aplicativo não pôde identificar os blocos que foram usados ou alterados na máquina virtual. Esse problema pode ocorrer quando o sistema ESX Server é reiniciado enquanto a máquina virtual está em execução. Na próxima vez que uma tarefa de backup for executada, o aplicativo redefinirá o rastreamento do bloco alterado e executará um backup de verificação.
```

Solução:

Para corrigir esse comportamento, execute uma operação de consolidação do disco na máquina virtual. Para realizar a consolidação do disco, siga estas etapas.

1. Abra o VMware VI Client.
2. Expanda o sistema ESX Server da máquina virtual afetada.
3. Clique com o botão direito do mouse na máquina virtual afetada, selecione o instantâneo e clique em Consolidar no menu pop-up para consolidar os discos.
4. Envie a tarefa de backup novamente.

Não é possível abrir o arquivo VMDK

Válido em plataformas Windows.

Sintoma:

AS diversas tarefas simultâneas de backup falham no modo de transporte NDB (ou LAN). A seguinte mensagem é exibida no log de atividades:

```
Não é possível abrir o arquivo VMDK
```

Solução:

Essa é uma limitação de conexão do VMware. Os limites do protocolo NFC (Network File Copy) a seguir se aplicam:

- ESX 4: máximo de 9 conexões diretas
- ESX 4 pelo vCenter Server: máximo de 27 conexões
- ESXi 4: máximo de 11 conexões diretas
- ESXi 4 pelo vCenter Server: máximo de 23 conexões

As conexões não podem ser compartilhadas entre discos. Os limites máximo não se aplicam a conexões SAN e HOTADD. Se o cliente NFC não for desligado corretamente, as conexões podem permanecer abertas por dez minutos.

Os nós não aparecem na tela Nó após alterar o nome do nó

Válido em plataformas Windows.

Sintoma:

O nome do host do nó foi alterado depois que ele foi adicionado à tela Nó. O nó não será mais exibido na tela Nó.

Solução:

Esse comportamento é esperado. O CA ARCserve Central Host-Based VM Backup mantém o nome do nó que foi adicionado na tela Nó. Ao renomear o nó, o aplicativo não poderá detectá-lo. Do mesmo modo, o nó não será exibido na tela Nó.

Para exibir os nós renomeados na tela, proceda da seguinte maneira:

1. Renomeie o nó.
2. Abra a tela Nó e exclua o nó (na página 48) que foi renomeado.
3. Adicione o nó usando seu novo nome.

Ocorrem diversos erros de conexão ao salvar ou atribuir uma diretiva ao servidor do CA ARCserve D2D

Válido em todas as plataformas Windows.

Sintoma:

Ao tentar salvar ou atribuir uma diretiva a um servidor do CA ARCserve D2D, a mensagem de erro a seguir é exibida:

```
Falha ao validar o destino do backup. Não são permitidas várias conexões com um servidor ou recurso compartilhado pelo mesmo usuário, usando mais de um nome de usuário. Desconecte todas as conexões anteriores com o servidor ou recurso compartilhado e tente novamente.
```

Solução:

Se a mensagem anterior for exibida ao tentar salvar ou atribuir uma diretiva a um servidor do CA ARCserve D2D, as seguintes ações corretivas pode ajudá-lo a resolver o problema:

- Marque o campo Nome de usuário com o nome do usuário\nome do computador (ou domínio).
- Vá para o servidor remoto onde a pasta compartilhada está hospedada e exclua todas as sessões do servidor do CA ARCserve Central Applications ou do servidor do CA ARCserve D2D. Siga um destes procedimentos para excluir as sessões:
  - Execute a linha de comando a seguir:

    ```
    net session \\machinename /delete
    ```
  - Vá para o seguinte diretório para desconectar a sessão:

    ```
    Compmgmt.msc > Ferramentas do sistema > Pastas compartilhadas > Sessões > Desconectar sessão
    ```
- Verifique se você está usando o mesmo nome de usuário para acessar a pasta compartilhada remota.
- Salve e implante a diretiva novamente.

Os backups da máquina virtual falham porque o ESX Server não está acessível

Válido em plataformas Windows.

Sintoma:

Os backups da máquina virtual falham. A seguinte mensagem é exibida no log de atividades:

```
Falha ao criar instantâneo da máquina virtual.
```

Solução:

Os backups de máquinas virtuais podem falhar ao executar vários backups simultaneamente em um sistema ESX Server. O problema não ocorrerá se vários backups forem executados simultaneamente em diferentes sistemas ESX Server. Para fazer backup de máquinas virtuais, o CA ARCserve Central Host-Based VM Backup captura um instantâneo dos dados que residam em máquinas virtuais. Quando várias operações de instantâneos são executadas simultaneamente em um sistema, o sistema ESX Server poderá ficar inoperante. Embora o tempo em que o ESX Server fica inoperante é temporário, a operação de backup será interrompida o que faz com que o backup falhe.

Para evitar que os backups falhem, use a solução apropriada para o seu ambiente:

- Reduza a quantidade de máquinas virtuais que estão fazendo backup simultaneamente. Por exemplo, se você estiver fazendo backup de oito máquinas virtuais simultaneamente, reduza a quantidade para sete máquinas virtuais, envie o backup novamente e, em seguida, analise os resultados. Se necessário, reduza a quantidade de máquinas virtuais que estão incluídas no backup até que os backups não falham ou a mensagem acima não apareça no Log de atividades.

  Para reduzir a quantidade de máquinas virtuais em um backup, cancele a atribuição de máquinas virtuais da diretiva. Para obter mais informações, consulte Cancelar a atribuição de diretivas de máquinas virtuais.

- Defina um limite para a quantidade de backups simultâneos. Essa abordagem ajuda a controlar a quantidade de tarefas de backup que podem ser executadas simultaneamente em seu ambiente. Para obter mais informações, consulte Definir um limite para a quantidade de backups simultâneos (na página 184).

O link Adicionar nova guia não é iniciado corretamente no Internet Explorer 8 e 9 nem no Chrome

Válido no Windows

Sintoma:

Ao adicionar o link de uma nova guia à barra de navegação especificando o URL de um HTTPS, as seguintes mensagens de erros serão exibidas quando eu clicar na nova guia:

- Internet Explorer 8 e 9:

  `O conteúdo foi bloqueado porque não foi assinado por um certificado de segurança válido.`

- Chrome:

  `Esta página web não está disponível.`

Solução:

Para corrigir esse problema no Internet Explorer, faça o seguinte:

- Internet Explorer 8:

  Clique na barra de mensagens e selecione "Exibir Conteúdo Bloqueado".

- Internet Explorer 9:

  Clique no botão "Mostrar conteúdo" na barra de mensagens na parte inferior da página. A página é atualizada e o link para a guia adicionada é aberto com êxito.

Para corrigir esse problema no Chrome, execute as seguintes etapas:

Etapa 1 - Exportar certificado:

1. Abra uma nova guia no Chrome e digite o URL do HTTPS.

   A mensagem de aviso "The site's security certificate is not trusted!" é exibida.

2. Na barra de endereços, clique no cadeado com 'X'.

   Uma janela pop-up é exibida com o link Certification Information.

3. Clique nesse link.

   A caixa de diálogo Certificate é aberta.

4. Clique na guia Details e, em seguida, clique em Copy to File, para salvar o certificado em seu computador local.

   A caixa de diálogo do Assistente para exportação de certificados é exibida.

5. Clique em Next para selecionar o formato deseja usar para exportar o arquivo.

   Observação: o binário X.509 codificado por DER (*.CER) vem selecionado por padrão.

6. Clique em Next para ir para o local em que deseja salvar o certificado.
7. Clique em Next para concluir o Certificate Export Wizard e, em seguida, clique em Finish.

O certificado é exportado com êxito.

Etapa 2 - Importar certificado:

1. Abra a caixa de diálogo Tools Options no Chrome.

   A tela Options é aberta.

2. Selecione a opção Under the Hood e clique em Manage Certificates from HTTPS/SSL.

   A caixa de diálogo Certificates é aberta.

3. Clique em Importar.

   A caixa de diálogo do Assistente para importação de certificados é exibida.

4. Clique em Next para ir para o certificado salvo no seu computador local.
5. Clique em Avançar para abrir o Armazenamento de certificados.

   A caixa de diálogo Certificate Store é aberta.

6. Clique em Browse para abrir a caixa de diálogo Select Certificate Store.

   A caixa de diálogo Select Certificate Store é aberta.

7. Selecione as Trusted Root Certification Authorities na lista de arquivos e clique em OK.

   A caixa de diálogo Armazenamento de certificados é aberta.

8. Clique em Next para concluir o Certificate Import Wizard e, em seguida, clique em Finish.

   A caixa de diálogo Security Warning é exibida, indicando que você está prestes a instalar um certificado.

   Clique em Sim para concordar com os termos.

O certificado é importado com êxito.

O link Adicionar nova guia, os feeds de RSS e os comentários de rede social não são iniciados corretamente no Internet Explorer 8 e 9

Válido no Windows

Sintoma:

Para o URL de um HTTPS do CA ARCserve Central Applications:

Ao adicionar o link de uma nova guia à barra de navegação especificando o URL de um HTTP, as seguintes mensagens de erro serão exibidas quando eu clicar na nova guia e no link Comentários:

```
A navegação para a página da web foi cancelada.
```

Além disso, os feeds de RSS não são exibidos.

Observação: o link Comentários também exibe a mensagem de erro, mesmo que você não selecione o link da nova guia.

Solução:

Para resolver esse problema, faça o seguinte:

- Internet Explorer 8:

  Após efetuar logon, clique em Não na mensagem pop-up de aviso de segurança, "Deseja exibir apenas o conteúdo oferecido de forma segura por esta página da Web?". Clicar em Não permite a entrega de conteúdo que não seja seguro em sua página da web.

- Internet Explorer 9:

  Clique no botão "Mostrar todo o conteúdo" na barra de mensagens na parte inferior da página. A página é atualizada e o link da guia adicionada é aberto com êxito.

Não é possível especificar um asterisco ou caractere sublinhado como um caractere curinga nos campos do filtro usando um teclado japonês

Válido no Windows

Sintoma:

Devido à diferença entre o teclado dos EUA e o japonês, não é possível digitar o caractere curinga "*" e outros caracteres especiais no teclado japonês, como o caractere sublinhado "_", nos campos de filtro a seguir:

- Ocorre apenas no Firefox:
  - Nó > Adicionar grupo - campo Filtragem pelo nome do nó
  - Políticas > guia Atribuição de diretiva > Diretiva a ser atribuída ou ter a atribuição cancelada - campo Filtragem pelo nome do nó
  - Restaurar > Explorador de nós - campo Nome do nó
  - Nó > Adicionar nós a partir do resultado da detecção automática > Nós para proteger - campo Nome do nó

Solução:

Para evitar que isso ocorra, abra um aplicativo de edição de texto, como o Bloco de notas. Digite os caracteres especiais, como "*" e "_", no editor de texto. Em seguida, copie os caracteres do editor de texto no campo.

A recuperação de uma máquina virtual usa um modo de transporte diferente do especificado

Válido em plataformas Windows.

Sintoma:

A recuperação da máquina virtual usará outro modo de transporte que o especificado na chave de registro.

Solução:

Esse comportamento afeta os discos delgados. Para corrigir este problema, siga estas etapas:

1. Efetue logon no sistema de proxy de backup do CA ARCserve D2D para as máquinas virtuais.
2. Abra o editor de registro e procure a seguinte chave:

   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFRestoreDll
3. Defina a chave de registro EnforceTransportForRecovery para um dos seguintes modos de transporte:
   - NBD
   - NBDSSL
4. Enviar a recuperação da máquina virtual.

O CA ARCserve Central Host-Based VM Backup não reconhece os volumes nos discos dinâmicos ao recuperar a máquina virtual em um ESX Server ou Hyper-V Server alternativo

Válido em plataformas Windows.

Sintoma:

O aplicativo não consegue reconhecer os volumes nos discos dinâmicos ao recuperar a máquina virtual em um ESX Server ou Hyper-V Server alternativo.

Alguns dos discos se tornam offline e os volumes correspondentes se tornam indisponíveis quando a máquina virtual é iniciada.

Solução:

Para recuperar os volumes, efetue logon na máquina virtual em modo de espera e defina manualmente os discos online no diskmgmt.msc.

Restaurar problemas de dados quando os dados são copiados em backup usando o modo de transporte HotAdd para discos maiores que 2 TB no Tamanho

Sintoma:

Ao fazer o backup de arquivos VMDK (Virtual Machine Disk – Disco da Máquina Virtual) com mais de 2 TB em tamanho usando o modo de transporte do VMware HotAdd, o backup é bem-sucedido mas os dados restaurados estão corrompidos.

Solução:

Devido a um problema conhecido do VMware VDDK (Virtual Disk Development Kit), a tarefa de backup é bem-sucedida mas os dados restaurados estão corrompidos. Para solucionar esse problema, execute uma das seguintes tarefas:

- Reconfigurar o plano de backup para permitir que a tarefa de backup seja executada em um proxy de backup diferente, que não seja executada usando o modo de transporte HotAdd.
- Definir as configurações do registro para garantir que o modo de transporte usado durante o backup não seja HotAdd. É possível usar SAN ou NBD/NBDSSL.

Para obter mais informações sobre esse problema do VMware, consulte a Documentação do VMware http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2068424.

Capítulo 6: Aplicando práticas recomendadas

Esta seção contém os seguintes tópicos:

Executar recuperação bare metal de uma máquina virtual

A Recuperação bare metal é suportada quando uma máquina virtual está ligada no momento em que a tarefa de backup é executada.

A BMR (Bare Metal Recovery - Recuperação Bare Metal) é o processo de restauração de um sistema de computador a partir do estado bare metal, incluindo a reinstalação do sistema operacional e dos aplicativos de software e, em seguida, a restauração dos dados e das configurações. O processo de BMR permite a restauração completa de um computador com o mínimo de esforço, até mesmo para um hardware diferente. A BMR é possível porque durante o processo de backup em nível de bloco, o CA ARCserve D2D não captura apenas os dados, mas também todas as informações relacionadas a:

- Sistema operacional
- Aplicativos instalados
- Configurações
- Drivers necessários

Para todas as informações relevantes, necessárias à execução de uma recompilação completa do sistema a partir do estado bare metal, é feito backup em uma série de blocos, os quais são armazenados no local do backup.

CA Support: Como: executar uma recuperação bare metal

YouTube: Como: executar uma recuperação bare metal

Antes de executar a BMR, é preciso ter:

- Um dos seguintes itens:
  - Uma imagem ISO criada da BMR gravada em um CD/DVD
  - Uma imagem ISO criada da BMR gravada em um dispositivo USB portátil

  Observação: o CA ARCserve D2D usa o utilitário do kit de inicialização para combinar uma imagem do WinPE e uma imagem do CA ARCserve D2D a fim de criar uma imagem ISO da BMR. Em seguida, essa imagem ISO é gravada em uma mídia inicializável. Dessa maneira, você pode usar qualquer uma dessas mídias inicializáveis (CD/DVD ou dispositivo USB) para inicializar o novo sistema do computador e permitir que o processo de recuperação bare metal seja iniciado. Para garantir que a imagem salva seja sempre a versão mais atualizada, é uma boa prática criar uma nova imagem ISO sempre que você atualizar o CA ARCserve D2D.

- Ao menos um backup completo disponível.
- Uma RAM de ao menos 1 GB instalada na máquina virtual e o servidor de origem que se está recuperando.
- Para recuperar máquinas virtuais VMware para máquinas virtuais VMware configuradas para se comportarem como servidores físicos, verifique se o VMware Tools está instalado na máquina virtual de destino.

Discos dinâmicos serão restaurados somente no nível do disco. Se o backup dos dados for feito no volume local de um disco dinâmico, você não poderá restaurar este disco durante a BMR. Nesse cenário, para fazer uma restauração durante uma BMR, é preciso executar uma das tarefas abaixo e, em seguida, realizar a BMR a partir do ponto de recuperação copiado:

- Faça backup em um volume em outra unidade.
- Faça backup em um compartilhamento remoto.
- Copie um ponto de recuperação em outro local.

Observação: se você executar uma BMR com vários discos dinâmicos, ela pode falhar devido a alguns erros inesperados (como falha na inicialização, volumes dinâmicos não reconhecidos e assim por diante). Se isso ocorrer, será necessário restaurar somente o disco do sistema usando a BMR e, em seguida, após a reinicialização do computador, será possível restaurar os outros volumes dinâmicos em um ambiente normal.

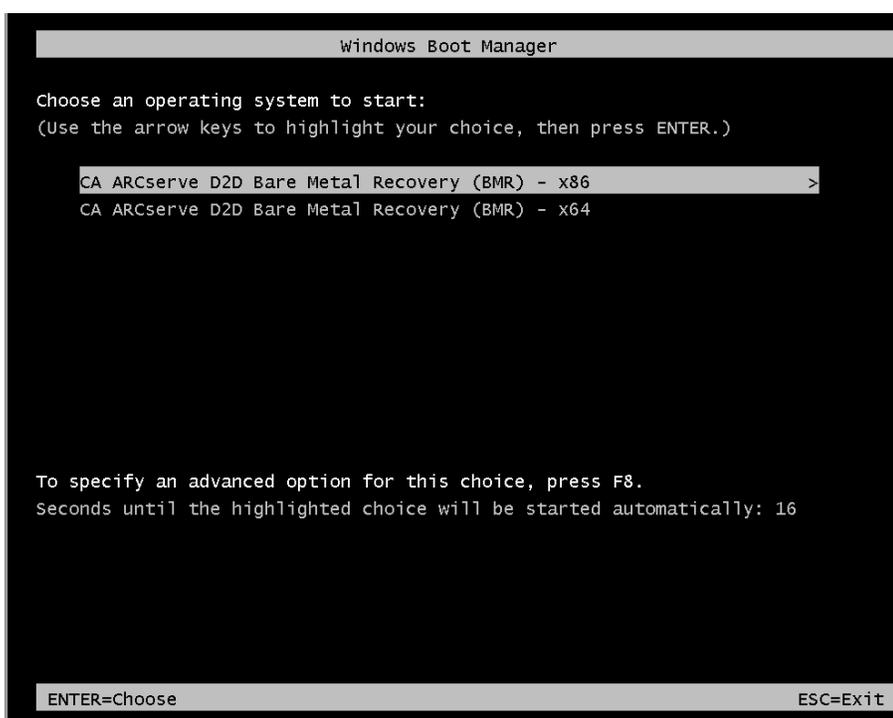
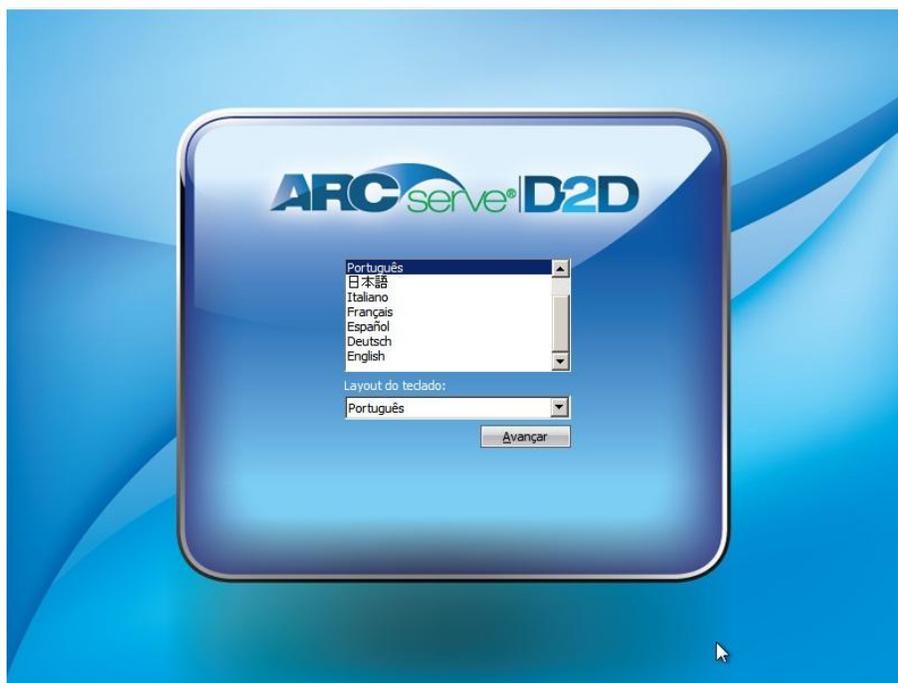
Independentemente do método usado para criar a imagem do kit de inicialização, o processo de BMR é basicamente o mesmo.

Observação: não é possível criar espaços de armazenamento por meio do processo de BMR. Se o computador de origem tinha espaço de armazenamento, não será possível criar espaços de armazenamento no computador de destino durante a BMR. Você pode restaurar os volumes em discos/volumes regulares ou criar manualmente espaços de armazenamento antes de executar a BMR e, em seguida, restaurar os dados nesses espaços de armazenamento criados.

Para restaurar dados usando a recuperação bare metal:

1. Insira a mídia da imagem do kit de inicialização salva e inicialize o computador.
   - Se estiver usando uma imagem ISO da BMR gravada em um CD/DVD, insira o CD/DVD.
   - Se estiver usando uma imagem ISO da BMR gravada em um dispositivo USB, insira o dispositivo USB.

   A tela do utilitário de instalação do BIOS é exibida.

2. Na tela do utilitário de instalação do BIOS, selecione a opção da unidade de CD-ROM ou a opção de USB para iniciar o processo de inicialização. Selecione uma arquitetura (x86/x64) e pressione Enter para continuar.

3. A tela de seleção de idioma do CA ARCserve D2D é exibida. Selecione um idioma e clique em Avançar para continuar.

O processo de recuperação bare metal é iniciado, e a tela do assistente da BMR inicial é exibida.

BMR (Bare Metal Recovery - Recuperação Bare Metal) do CA ARCserve D2D
- Escolha um tipo de BMR

Especifique um tipo de recuperação:

◉ **Recuperar dados cujo backup foi feito usando o CA ARCserve D2D**

(Sessões de backup usando o CA ARCserve D2D ou CA ARCserve Central Host-Based VM Backup).

○ **Recuperar usando uma VM no modo de espera virtual do Hyper-V**

(é possível recuperar dados apenas se a conversão virtual tiver sido feita usando o CA ARCserve Central Virtual Standby)

○ **Recuperar usando uma VM no modo de espera virtual do VMware**

(é possível recuperar dados apenas se a conversão virtual tiver sido feita usando o CA ARCserve Central Virtual Standby)

4. Na tela Assistente para BMR, selecione o tipo de BMR que deseja executar:

   - **Recuperar dados armazenados em backup usando o CA ARCserve D2D**

     Permite a recuperação de dados cujo backup foi feito usando o CA ARCserve D2D. Essa opção é usada juntamente com sessões de backup realizadas com o CA ARCserve D2D ou com o aplicativo CA ARCserve Central Host-Based VM Backup.

     Se selecionar essa opção, continue este procedimento a partir daqui.

   - **Recuperar usando uma VM no modo de espera virtual do Hyper-V**

     Permite recuperar dados de uma máquina virtual cuja conversão é executada em uma máquina virtual do Hyper-V. Essa opção é usada juntamente com o aplicativo do CA ARCserve Central Virtual Standby.

     Observação: para essa opção, só é possível recuperar dados se a conversão virtual para um arquivo VHD (para Hyper-V) foi executada usando o CA ARCserve Central Virtual Standby.

     Se selecionar essa opção, consulte o tópico Recuperar usando uma VM no modo de espera virtual do Hyper-V para continuar com este procedimento.

   - **Recuperar usando uma VM no modo de espera virtual do VMware**

     Permite recuperar dados de uma máquina cuja conversão virtual é executada em uma máquina virtual do VMware.   Essa opção é usada juntamente com o aplicativo do CA ARCserve Central Virtual Standby.

     Observação: para essa opção, só é possível recuperar dados se a conversão virtual para um arquivo VMDK (para VMware) foi executada usando o CA ARCserve Central Virtual Standby.

     Se selecionar essa opção, consulte o tópico Recuperar usando uma VM no modo de espera virtual do VMware para continuar com este procedimento.

5. Clique em Avançar.

   A tela do assistente Selecionar um ponto de recuperação é exibida.

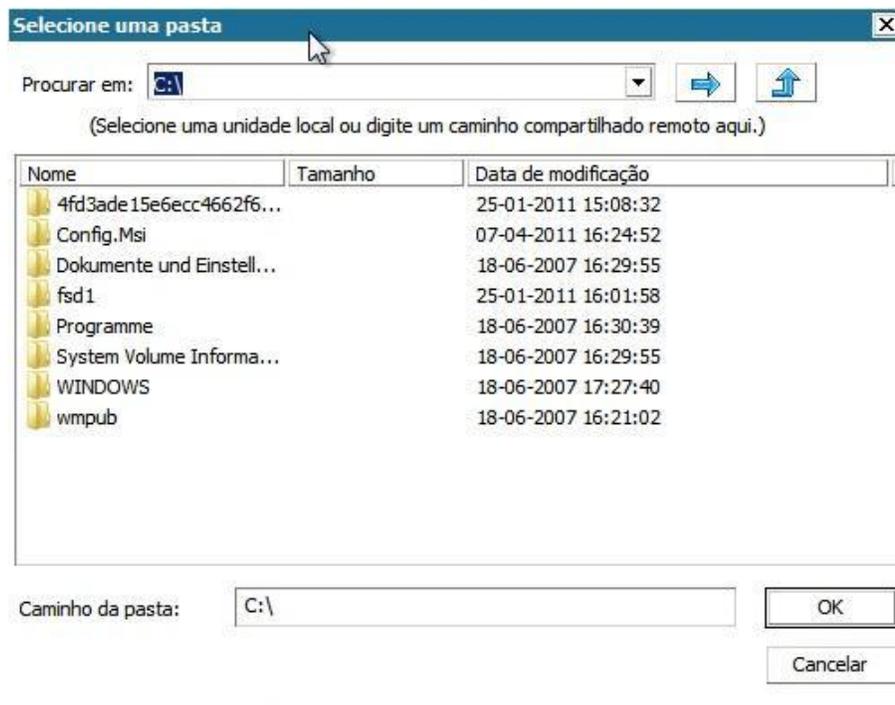
6. Nesta tela, selecione o computador (ou volume) que contenha pontos de recuperação para a imagem de backup.

   O CA ARCserve D2D permite recuperar a partir de uma unidade local ou compartilhamento de rede.

   - Se você estiver recuperando a partir de um backup local, o assistente de BMR detectará e exibirá automaticamente todos os volumes contendo pontos de recuperação.
   - Caso esteja fazendo uma recuperação a partir de um compartilhamento remoto, procure o local remoto em que os pontos de recuperação estão armazenados. Se houver vários computadores contendo pontos de recuperação, todos eles serão exibidos.

     Você também pode precisar acessar informações (nome de usuário e senha) para o computador remoto.

     Observação: a rede deve estar em funcionamento para procurar pontos de recuperação. Se necessário, você pode verificar e atualizar as informações de configuração de rede ou carregar qualquer driver ausente do menu Utilitários.

7. Se o módulo de BMR não puder detectar nenhum volume de destino local, a caixa de diálogo Selecione uma pasta é exibida automaticamente. Forneça o compartilhamento remoto em que os backups residem.

8. Selecione a pasta onde estão armazenados os pontos de recuperação para backup e clique em OK. (Pode-se clicar no ícone de seta verde para validar a conexão com o local especificado.)

   A tela do assistente de BMR agora exibe as seguintes informações:

   - Nome da máquina (no painel superior à esquerda).
   - Informações relacionadas ao backup (no painel superior à direita).
   - Todos os pontos de recuperação correspondentes (no painel inferior à esquerda).

   Observação: para sistemas operacionais com suporte, é possível realizar uma BMR a partir de um backup executado em um computador UEFI para um computador compatível com o BIOS e a partir de um computador BIOS para um computador compatível com a UEFI. Consulte Sistemas operacionais que oferecem suporte à conversão de UEFI/BIOS para obter uma lista completa de sistemas de conversão de firmware com suporte.

     - Em sistemas operacionais que não oferecem suporte à conversão de firmware, para executar uma BMR para um sistema UEFI, você deve inicializar o computador no modo UEFI. A BMR não oferece suporte a restauração de um computador com firmware diferente. Para verificar se o firmware de inicialização é UEFI e não BIOS, clique em Utilitários, Sobre.
     - Em sistemas operacionais que oferecem suporte à conversão de firmware, após selecionar um ponto de recuperação, e se for detectado que o computador de origem não é o mesmo firmware que seu sistema, você será indagado se deseja converter a UEFI em um sistema compatível com o BIOS ou o BIOS em um sistema compatível com a UEFI.

ARCserve D2D Bare Metal Recovery

BMR (Bare Metal Recovery - Recuperação Bare Metal) do CA ARCserve D2D
- Selecionar ponto de recuperação

O painel superior exibe todos os computadores armazenados em backup e os destinos de seus backups. Ao clicar em um computador, você poderá ver os pontos de recuperação associados no painel inferior. Selecione um ponto de recuperação para continuar.

Observação: por padrão, apenas os computadores armazenados em backup detectados a partir de volumes locais são relacionados aqui. Depois que um novo disco removível é conectado ou desconectado, clique em "Atualizar" para atualizar a lista de computadores.
Você também pode clicar em "Procurar" para adicionar qualquer computador armazenado em backup a partir da pasta compartilhada remota.

Se você não conseguir procurar a pasta

1 adaptador(es) de rede detectado(s)
Intel(R) PRO/1000 MT Network Connection
- Endereço IP: 155.35.128.89
- Status: Conectado

Foram detectados os seguintes computadores armazenados em backup:

Informações armazenadas em backup
Nome do host:
Sistema operacional: Windows 7
Plataforma: X64

Atualizar | Procurar

Selecione abaixo um dos pontos de recuperação detectados para o computador especificado e continue:

17-04-2012
01:17:52
00:44:54
16-04-2012
11-04-2012

Tipo de backup:
- Backup de verificação
Destino do backup (detectado no sistema atual):
-
Descrição do backup:
- Backup de verificação personalizado
Firmware de inicialização:
- UEFI
Recuperação bare metal do CA ARCserve D2D pa

Utilitários | Voltar | Avançar | Cancelar

9. Selecione o ponto de recuperação a ser restaurado.

   As informações relacionadas ao ponto de recuperação selecionado são exibidas (no painel inferior à direita). Essa exibição inclui informações como o tipo de backup executado (e salvo), o destino do backup e os volumes incluídos no backup.

   Se o ponto de recuperação contiver sessões criptografadas (o ícone de relógio do ponto de recuperação terá um cadeado), uma tela de senha obrigatória será exibida. Digite a senha da sessão e clique em OK.

   Observação: se seu computador for um controlador de domínio, o CA ARCserve D2D oferece suporte a uma restauração não autoritativa do arquivo de banco de dados do AD (Active Directory) durante a BMR. (O CA ARCserve D2D não oferece suporte à restauração de agrupamentos do MSCS.)

10. Verifique o ponto de recuperação que deseja restaurar e clique em Avançar.

    Uma tela do assistente de BMR é exibida com as opções disponíveis do modo de recuperação.

11. Selecione o modo de recuperação.

    As opções disponíveis são Modo avançado e Modo expresso.

    - Selecione o Modo avançado, caso deseje personalizar o processo de recuperação.
    - Selecione o Modo expresso, se desejar o mínimo de interação durante o processo de recuperação.

    Padrão: Modo expresso.

    Observação: o restante desse procedimento é aplicável apenas se o modo avançado for selecionado e se o procedimento fornecer informações para orientá-lo durante o processo da BMR.

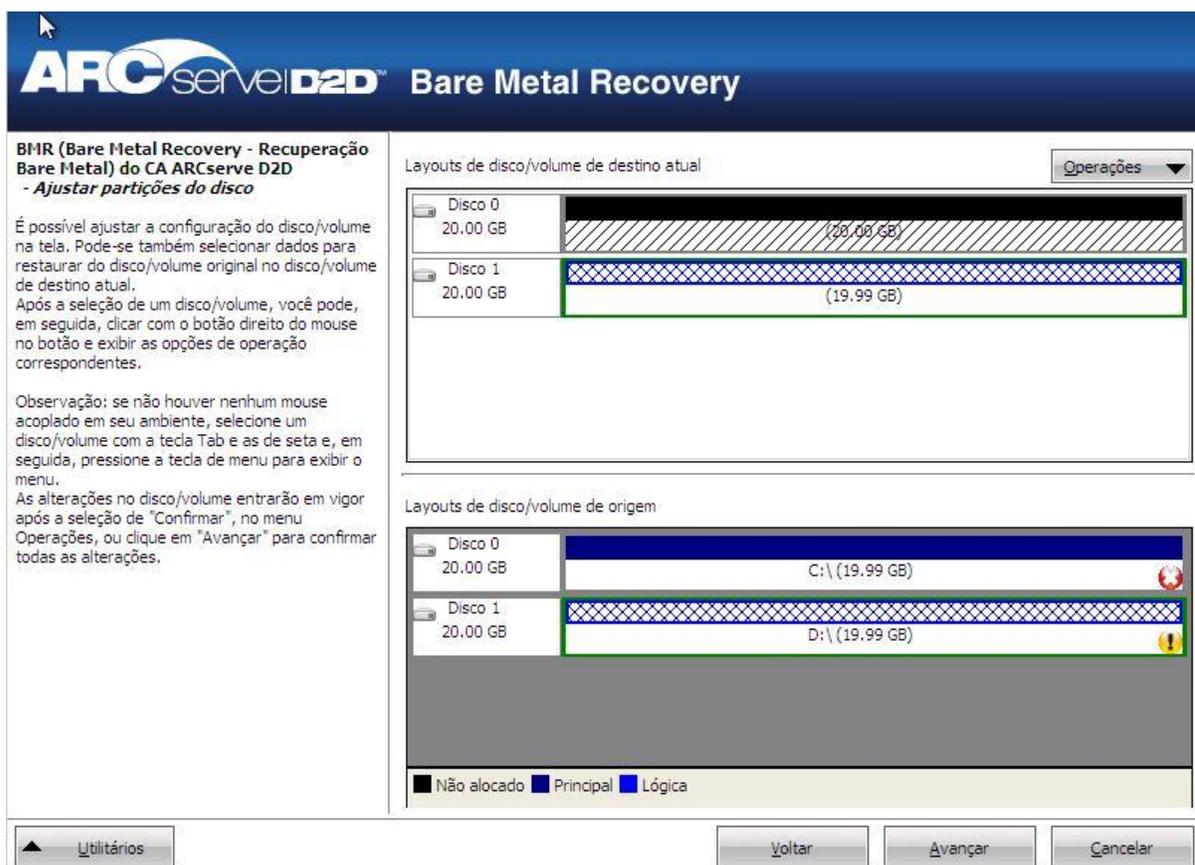
12. Clique em Avançar.

    O utilitário BMR inicia localizando o computador a ser recuperado e exibe as informações da partição de disco correspondente.

    O painel superior mostra a configuração de disco que você possui no computador atual (destino) e o painel inferior mostra as informações da partição de disco que havia no computador original (origem).

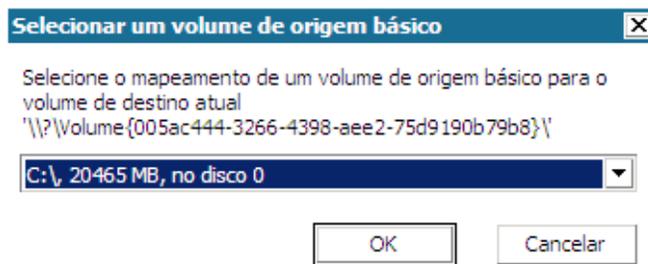
    Importante: Um ícone vermelho em forma de X exibido para um volume de origem no painel inferior indica que o volume contém informações do sistema e não foi atribuído (mapeado) ao volume de destino. O volume contendo informações do sistema do disco de origem deve ser atribuído ao disco de destino e restaurado durante a BMR, caso contrário, haverá falha na reinicialização.

    Observação: se executar a BMR e restaurar o volume do sistema em um disco que não está configurado como disco de inicialização, haverá falha ao iniciar o computador após o término da BMR. Verifique se está restaurando o volume do sistema em um disco de inicialização configurado corretamente.

    Observação: ao restaurar em outro disco/volume, a capacidade do novo disco/volume deve ser do mesmo tamanho ou maior do que o disco/volume original. Além disso, o redimensionamento do disco destina-se somente a discos básicos, não a discos dinâmicos.

13. Se as informações do disco atual que você estiver vendo não parecem corretas, acesse o menu Utilitários e verifique se há drivers ausentes.

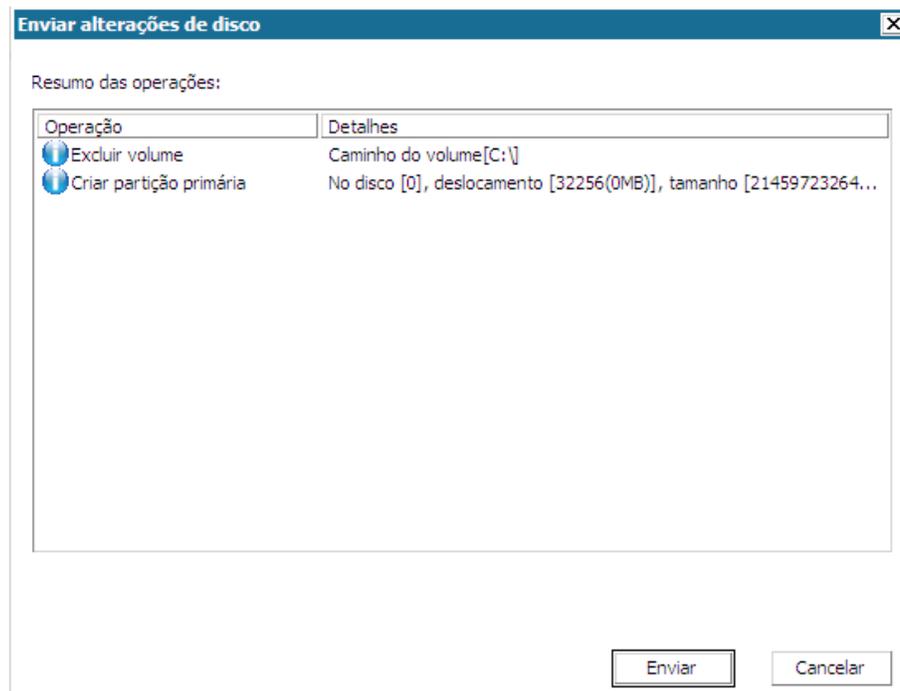
14. Se necessário, no painel de disco/volume de destino, clique no menu suspenso Operações para exibir as opções disponíveis. Para obter mais informações sobre essas opções, consulte Gerenciando o menu operações de BMR.

15. Clique em cada volume de destino e, no menu pop-up, selecione a opção Mapear volume de para atribuir um volume de origem a este volume de destino.

    A caixa de diálogo Selecionar um volume de origem básico é exibida.

16. Nesta caixa, clique no menu suspenso e selecione o volume de origem disponível para atribuí-lo ao volume de destino selecionado. Clique em OK.

    - No volume de destino, um ícone de marca de seleção é exibido, indicando que o volume de destino foi mapeado.
    - No volume de origem, o ícone em forma de X vermelho muda para verde, indicando que o volume de origem foi atribuído a um volume de destino.

17. Quando tiver certeza de que todos os volumes que desejar restaurar e todos os volumes que tiverem informações do sistema foram atribuídos a um volume de destino, clique em Avançar.

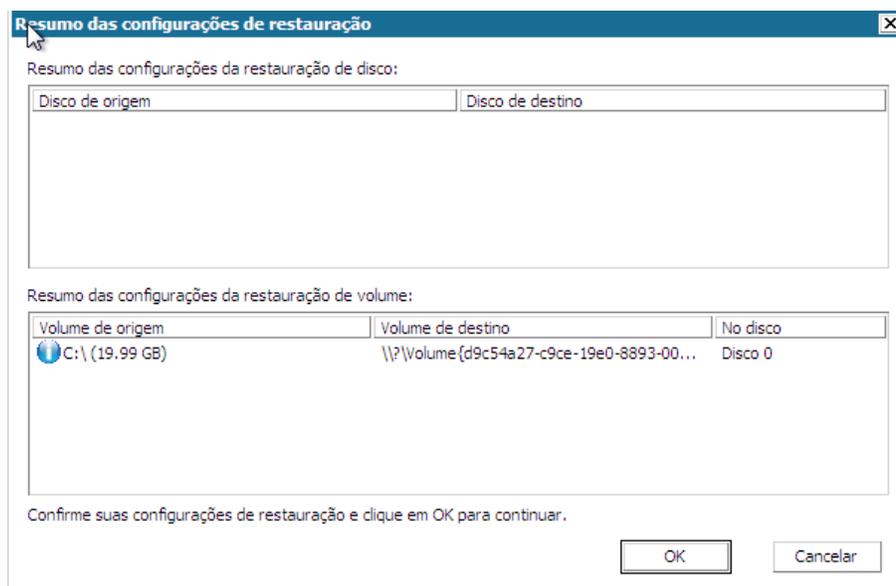
    A tela Enviar alterações de disco é exibida, mostrando um resumo das operações selecionadas. Para cada novo volume criado, são exibidas as informações correspondentes.

18. Ao confirmar se as informações de resumo estão corretas, clique em Enviar. (Se não estiverem corretas, clique em Cancelar.)

    Observação: as operações no disco rígido não entrarão em vigor até que sejam enviadas.

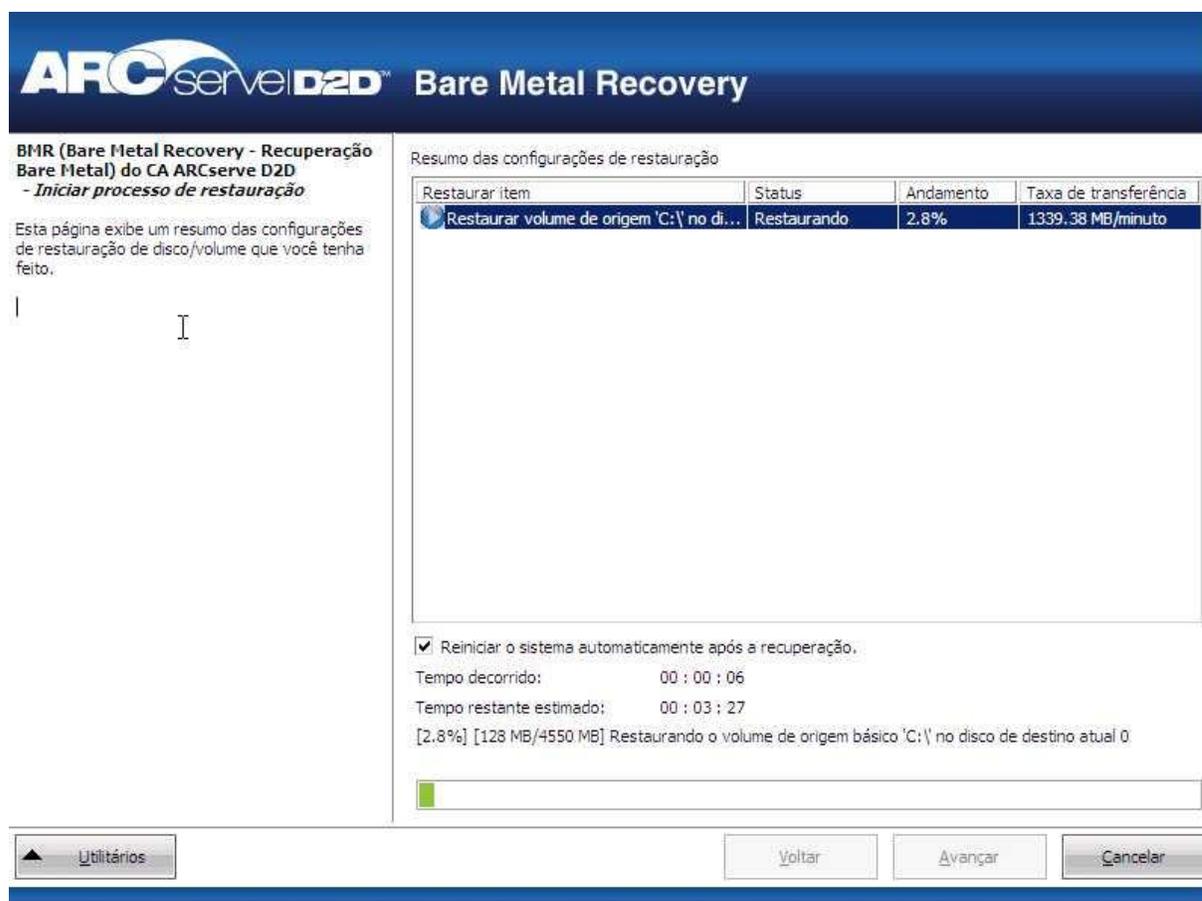
    No computador de destino, os novos volumes são criados e mapeados para o computador de origem correspondente.

19. Quando as alterações forem concluídas, clique em OK.

    A tela Resumo das configurações de restauração é exibida, mostrando um resumo dos volumes a serem restaurados.

    Observação: na parte inferior da janela de resumo da restauração, as letras de unidade listadas na coluna Volume de destino são geradas automaticamente no WinPE (Windows Preinstallation Environment - Ambiente de Pré-Instalação do Windows). Elas podem ser diferentes das listadas na coluna Volume de origem. No entanto, os dados serão restaurados no volume apropriado, mesmo quando as letras forem diferentes.

20. Após verificar se as informações de resumo estão corretas, clique em OK.

    O processo de restauração é iniciado. A tela do assistente de BMR exibe o status da restauração para cada volume.

    - Dependendo do tamanho do volume sendo restaurado, essa operação pode levar algum tempo.
    - Durante este processo, você estará restaurando bloco por bloco tudo o que tiver sido armazenado em backup para esse ponto de recuperação e criando uma réplica do computador de origem no computador de destino.
    - Por padrão, a opção que permite reiniciar o sistema automaticamente depois da recuperação é selecionada. Se necessário, você pode desmarcar esta opção e reinicializar manualmente mais tarde.
    - Se necessário, é possível cancelar ou anular a operação a qualquer momento.

21. No menu Utilitários, é possível acessar o Log de atividades da BMR e usar a opção Salvar para salvar o Log de atividades.

    Por padrão, o log de atividades será salvo no seguinte local:

    X:\windows\system32\dr\log.

    Observação: para evitar um erro gerado pelo Windows, não salve o Log de atividades na área de trabalho nem crie uma nova pasta na área de trabalho usando a opção Salvar como, na janela Log de atividades da BMR.

22. Caso esteja restaurando em diferentes tipos de hardware (o adaptador SCSI/FC usado para conectar unidades de disco rígido pode ter sido alterado) e nenhum driver compatível tenha sido detectado no sistema original, uma página de injeção de drivers será exibida para permitir o fornecimento de drivers a esses dispositivos.

    Procure e selecione os drivers a serem injetados no sistema recuperado de forma que, mesmo se estiver fazendo a recuperação em um computador com tipos diferentes de hardware, ainda seja possível trazer o computador de volta após a BMR.

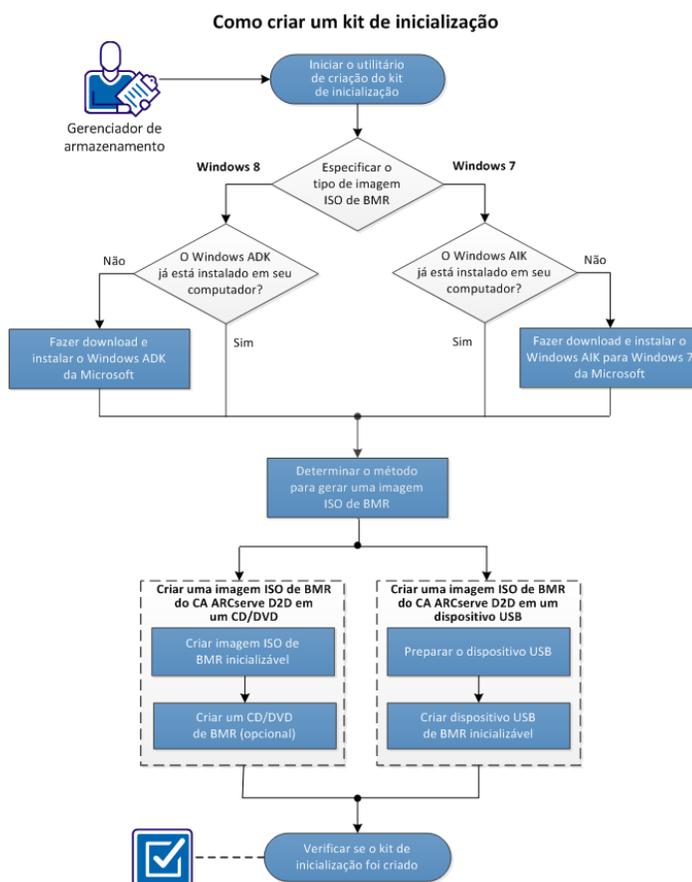
23. Quando o processo de BMR for concluído, uma notificação de confirmação é exibida.

Observações: após a conclusão da BMR:

- O primeiro backup realizado é o Backup de verificação.
- Verifique se a BIOS está configurada para inicializar a partir do disco no qual o volume de inicialização foi restaurado.
- Após a reinicialização do computador, talvez seja necessário configurar os adaptadores de rede manualmente caso você tenha restaurado em um hardware diferente.
- Quando o computador for reinicializado, uma tela de recuperação de erro do Windows pode ser exibida indicando que o Windows não foi desligado corretamente. Se isso ocorrer, você poderá ignorar esse aviso com segurança e continuar para iniciar o Windows normalmente.
- Para discos dinâmicos, se o status do disco for offline, é possível alterá-lo manualmente para online na interface de gerenciamento de disco (acessado executando o utilitário de controle Diskmgmt.msc).
- Para discos dinâmicos, se os volumes dinâmicos estiverem em um status de falha de redundância, é possível sincronizar novamente os volumes na interface de gerenciamento de disco (acessado usando o utilitário de controle Diskmgmt.msc).

Como criar um kit de inicialização

O CA ARCserve D2D usa um utilitário de kit de inicialização para combinar uma imagem do WinPE (Windows Preinstallation Environment - Ambiente de Pré-Instalação do Windows) e uma imagem do CA ARCserve D2D a fim de criar uma imagem ISO da BMR. Em seguida, essa imagem ISO é gravada em uma mídia inicializável. Ao executar uma recuperação bare metal, a mídia de inicialização do CA ARCserve D2D (CD/DVD ou dispositivo USB) é usada para inicializar o novo sistema do computador e permitir que o processo de recuperação bare metal seja iniciado.

O diagrama a seguir ilustra o processo para criar um kit de inicialização:

Execute as tarefas a seguir para criar um kit de inicialização:

1. Iniciar o utilitário de criação do kit de inicialização (na página 173)
2. Determinar o método para gerar uma imagem ISO da BMR (na página 176)
3. Criar uma imagem ISO da BMR do CA ARCserve D2D para um CD/DVD (na página 177)
   a. Criar a imagem ISO da recuperação bare metal inicializável (na página 177)
   b. (opcional) Criar um CD/DVD de BMR (na página 179)
4. Criar uma imagem ISO da BMR do CA ARCserve D2D para um dispositivo USB (na página 180)
   a. Preparar o dispositivo USB (na página 181)
   b. Criar um dispositivo USB de BMR inicializável (na página 182)
5. Verificar se o kit de inicialização foi criado (na página 184)

VÍDEOS COMPLEMENTARES

Este procedimento contém um vídeo de instrução adicional. Selecione ou o <suporte> ou o YouTube como a origem para visualizar este vídeo. As versões dos vídeos do CA Support e YouTube são idênticas e somente a origem de exibição é diferente.

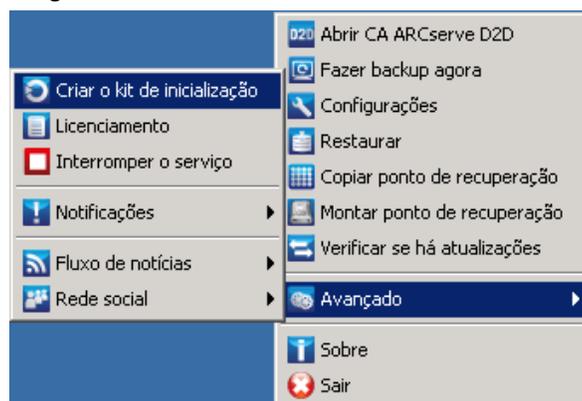
CA Support:	Como criar um kit de inicialização
YouTube:	Como criar um kit de inicialização

Iniciar o utilitário de criação do kit de inicialização

O CA ARCserve D2D fornece um utilitário de criação do kit de inicialização para recuperação bare metal a fim de ajudar você a gerar uma imagem ISO com base em WinPE. Essa imagem ISO contém todas as informações necessárias para a execução de uma BMR (Bare Metal Recovery - Recuperação Bare Metal), se necessário.

Siga estas etapas:

1. Você pode iniciar o utilitário Criar o kit de inicialização nas opções avançadas do monitor da bandeja do sistema ou no menu Iniciar.

   O utilitário de criação do kit de inicialização é iniciado, e a tela Especificar o tipo de imagem ISO da BMR é exibida.

2. Especifique o tipo de imagem ISO da BMR a ser criado (Windows 8 ou Windows 7) e clique em Avançar.

   Observação: o Windows XP, Windows Vista e Windows Server 2003 não são suportados para criar uma imagem ISO da BMR. Para esses sistemas operacionais, você pode usar o Windows Vista SP1, Windows 2003 SP2 ou uma versão posterior do Windows para criar sua imagem ISO da BMR.

   ■ **Windows 8**

     Quando iniciado, o utilitário imediatamente verifica o computador para determinar se o Windows ADK (Windows Assessment and Deployment Kit - Kit de Avaliação e Implantação do Windows) já está instalado. Microsoft Windows ADK é uma ferramenta da Microsoft que permite implantar os sistemas operacionais Windows em computadores.

     Observação: é possível instalar o Windows ADK em computadores com os seguintes sistemas operacionais em execução:

     - Windows 7
     - Windows Server 2008
     - Windows Server 2008 R2
     - Windows 8
     - Windows Server 2012

   ■ **Windows 7**

     Quando iniciado, o utilitário imediatamente verifica o computador para determinar se o Kit de Instalação Automatizada do Windows (AIK) já está instalado. Microsoft Windows AIK é uma ferramenta da Microsoft que permite implantar os sistemas operacionais Windows em computadores.

Observação: é possível instalar o Windows AIK para Windows 7 em computadores que executam os seguintes sistemas operacionais:

- Windows 2003 SP2
- Windows Vista SP1
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

3. Para criar a imagem ISO inicializável, o Windows ADK ou Windows AIK (conforme aplicável) deve estar instalado no computador.

    a. Se o Windows ADK (ou AIK) estiver instalado, o utilitário irá prosseguir para a tela Selecionar o método do kit de inicialização para que você possa continuar a criação do kit de inicialização.

    b. Se o Windows ADK (ou AIK) não estiver instalado, a respectiva tela de informações do Windows é aberta. É necessário fazer download e instalar o Windows ADK (ou AIK) do Centro de Download da Microsoft.

    Observação: para obter mais informações sobre como instalar o Windows ADK (ou AIK), consulte os seguintes sites:

    ■ Instalando o Windows ADK

    ■ Instalando o Windows AIK para Windows 7

    Você pode instalar o Windows ADK (ou AIK) usando um dos seguintes métodos:

    - Faça download da mídia de instalação diretamente do site da Microsoft e instale o Windows ADK (ou AIK) no computador.
    - Clique nos links na tela de informações para abrir o site da Microsoft, de forma que você possa fazer download do Windows ADK (ou AIK) e instalá-lo no computador.

      Depois de instalar o Windows ADK (ou AIK), clique em Avançar e o utilitário irá prosseguir para a tela Selecionar o método do kit de inicialização para permitir que você continue a criação do kit de inicialização.

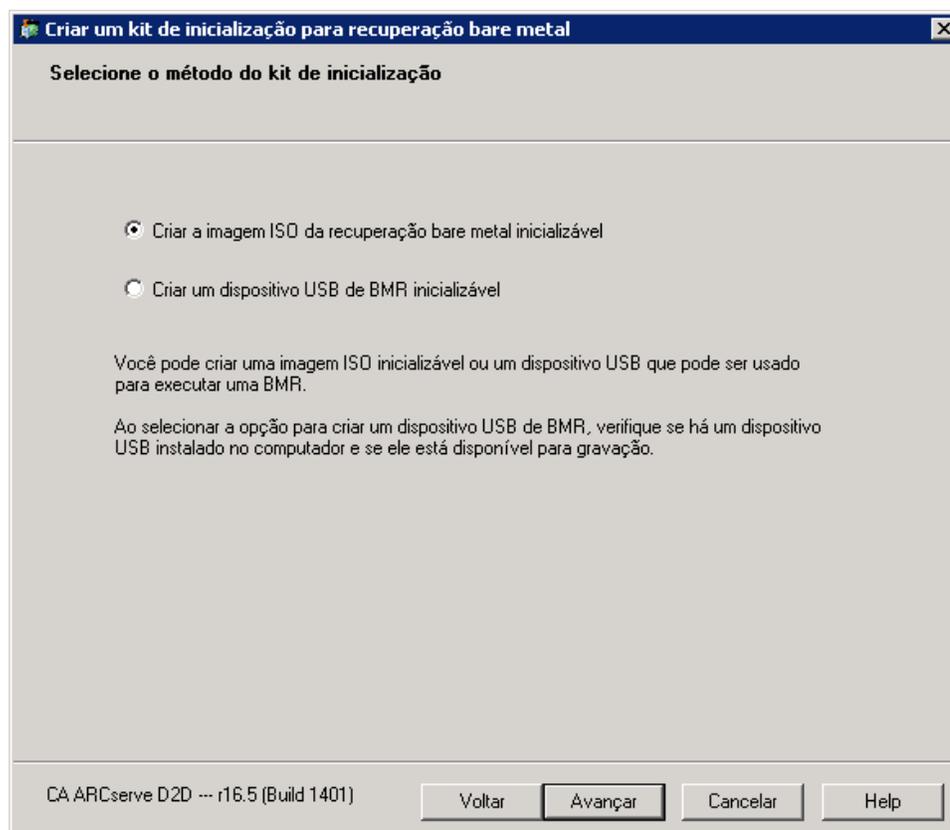
    Observação: para a instalação do Windows ADK, os seguintes recursos são necessários para suporte à criação do kit de inicialização:

    ■ Ferramentas de implantação

    ■ Ambiente de pré-instalação do Windows (Windows PE)

    Observação: para a instalação do Windows AIK, selecione a instalação do Windows AIK.

Determinar o método para gerar uma imagem ISO da BMR

O utilitário de criação do kit de inicialização oferece duas opções para gerar uma imagem ISO:

- Criar a imagem ISO da recuperação bare metal inicializável (na página 177)

  Esse método cria uma imagem ISO que pode ser gravada em um CD/DVD para armazenamento. Esta é a opção padrão. Para obter mais informações, consulte Criar uma imagem ISO da BMR do CA ARCserve D2D para um CD/DVD (na página 177).

- Criar um dispositivo USB de BMR inicializável (na página 182)

  Esse método cria uma imagem ISO e a grava diretamente em um dispositivo USB portátil para armazenamento. Para obter mais informações, consulte Criar uma imagem ISO da BMR do CA ARCserve D2D para um dispositivo USB (na página 180).

Você pode usar qualquer uma dessas mídias inicializáveis para inicializar o novo sistema do computador e permitir que o processo de recuperação bare metal seja iniciado. Para garantir que a imagem salva seja sempre a versão mais atualizada, é uma boa prática criar uma nova imagem ISO sempre que você atualizar o CA ARCserve D2D.

Observação: se estiver executando uma BMR em uma VM (Virtual Machine - Máquina Virtual), você também poderá vincular a imagem ISO à VM diretamente a fim de iniciar o processo de BMR sem ter de primeiro gravá-la em um CD/DVD.

Criar uma imagem ISO da BMR do CA ARCserve D2D para um CD/DVD

O processo para criar uma imagem ISO da BMR do CA ARCserve D2D consiste em:

- Criar a imagem ISO da recuperação bare metal inicializável (na página 177)
- Criar um CD/DVD de BMR (na página 179)

Criar a imagem ISO da recuperação bare metal inicializável

Se você optar por criar uma imagem ISO de BMR, é possível gravar essa imagem em uma mídia inicializável (CD ou DVD) para inicializar o novo sistema de computador e permitir que o processo de recuperação bare metal seja iniciado.

Siga estas etapas:

1. Na tela Selecionar o método do kit de inicialização, selecione Criar imagem ISO da BMR inicializável e clique em Avançar.

   A caixa de diálogo Selecionar a plataforma e o destino é aberta.

2. Selecione a plataforma aplicável para a imagem ISO.

   É possível selecionar qualquer uma das duas opções disponíveis, ou ambas. Se você selecionar as duas plataformas, isso resultará em tempo adicional para criar a imagem.

   Observação: uma imagem ISO criada a partir de uma plataforma de 32 bits deve ser usada para restaurar um servidor de 32 bits. Uma imagem ISO criada a partir de uma plataforma de 64 bits deve ser usada para restaurar um servidor de 64 bits. Se você deseja inicializar um sistema de firmware UEFI, certifique-se de que a opção de plataforma x64 esteja selecionada.

   As opções disponíveis são:

   - Imagem ISO da BMR para plataforma x86 (apenas).
   - Imagem ISO da BMR para plataforma x64 (apenas).
   - Imagem ISO da BMR para plataformas x86 e x64.

3. Especifique o destino.

   Especifique ou procure o local em que o arquivo de imagem ISO de BMR será criado e armazenado.

4. Especifique o nome do arquivo de imagem ISO de BMR gerado.

5. Depois de especificar a plataforma e o destino, clique em Avançar.

   A caixa de diálogo Selecionar idiomas é aberta.

6. Selecione o idioma para a imagem ISO de BMR gerada. Durante o procedimento de BMR, a interface do usuário e o teclado estarão integrados com o idioma selecionado.

   Você pode selecionar um ou mais idiomas diferentes para a imagem ISO de BMR. No entanto, cada idioma selecionado resultará em tempo adicional na criação da imagem. Quanto mais idiomas forem selecionados, maior será o tempo levado para a conclusão. Como resultado, você deve selecionar apenas os idiomas realmente necessários.

7. Clique em Avançar.

   A caixa de diálogo Especifique drivers é aberta.

8. Especifique os drivers para preencher a lista de drivers com drivers para serem integrados à imagem ISO da BMR.

   O painel de driver é ativado e é possível especificar todos os drivers adicionais que você deseja adicionar (ou excluir) da imagem ISO de BMR.

   Observação: ao integrar o VirtualBox Host-Only Ethernet Adapter Driver à imagem ISO da BMR, existe um possível conflito com os componentes do Windows ADK. Para evitar conflitos, a melhor prática é não integrar esse driver à imagem ISO da BMR.

   a. Incluir drivers locais: carregue os drivers de dispositivos críticos locais (somente drivers OEM para NIC, FC ou SCSI) à lista de drivers. Quando clicado, o utilitário verifica seu computador para determinar se há drivers de dispositivo críticos que precisam ser adicionados à imagem ISO da BMR para esse computador. Se quaisquer drivers de dispositivo críticos forem detectados, eles são automaticamente adicionados à lista.

   b. Adicionar driver: procure os drivers que você deseja que sejam adicionados à lista de drivers.

   c. Excluir driver: remova quaisquer drivers selecionados da lista que você não deseja que sejam adicionados à imagem ISO da BMR.

9. Clique em Criar para iniciar o processo e criar uma imagem ISO da BMR inicializável.

   Durante o processo, o status é exibido.

10. Quando o processo for concluído, uma tela de confirmação será exibida para indicar que a imagem ISO de BMR foi gerada com êxito. Essa tela também exibe o local e a plataforma da imagem, juntamente com um link clicável para navegar para esse local.

Criar um CD/DVD de BMR

Depois que a imagem ISO é criada e salva no destino especificado, você deve gravar a imagem em um CD ou DVD inicializável. Você pode usar essa mídia inicializável para inicializar o novo sistema de computador e permitir que o processo de recuperação bare metal seja iniciado.

Para garantir que a imagem ISO salva esteja sempre na versão mais atualizada:

- Você deve criar uma nova imagem ISO sempre que atualizar o CA ARCserve D2D.
- Se tiver salvado a imagem ISO em um local remoto, você deve gravar o CD/DVD apenas se for necessário executar uma BMR.
- Se o CA ARCserve D2D estiver instalado em vários computadores, você deve criar uma nova imagem ISO (e um CD/DVD correspondente) a partir de um computador válido antes da execução de uma BMR, de forma que a imagem inclua todas as atualizações do CA ARCserve D2D mais recentes.

Criar uma imagem ISO da BMR do CA ARCserve D2D para um dispositivo USB

O processo para criar um dispositivo USB de BMR do CA ARCserve D2D consiste em:

Preparar o dispositivo USB (na página 181)

Criar um dispositivo USB de BMR inicializável (na página 182)

Preparar o dispositivo USB

Antes de gravar a imagem ISO de BMR em um dispositivo USB, é necessário preparar o dispositivo. Para criar um dispositivo USB de BMR inicializável, o dispositivo deve ser ativado para permitir a inicialização do sistema. Você pode usar o comando DiskPart para tornar o dispositivo ativo.

Importante: se for necessário formatar o dispositivo USB, esse processo apagará todos os dados atualmente armazenados no dispositivo USB. Verifique se não há nada importante no dispositivo antes de executar esse processo. Se o dispositivo USB tiver sido previamente formatado, o processo substituirá todos os arquivos com nomes iguais.

Siga estas etapas:

1. Abra um prompt de comando (com direitos administrativos, se exigido por seu sistema operacional).
2. Digite **Diskpart** e pressione Enter.
3. Digite **List Disk** e pressione Enter.

   Uma listagem de todos os discos detectados é exibida. Determine qual dos discos exibidos é o seu disco USB.
4. Selecione o disco USB digitando **Select Disk <n>** ("n" é o número do disco USB) e pressione Enter.
5. Digite **Clean** e pressione Enter.

   O sistema exibirá DiskPart está limpando o disco.
6. Digite **create partition primary** e pressione Enter.

   O sistema exibirá DiskPart criou com êxito a partição especificada.
7. Digite **select partition 1** e pressione Enter.

   O sistema exibirá 1 é a partição selecionada.
8. Digite **active** e pressione Enter.

   O sistema exibirá O DiskPart marcou a partição atual como ativa.
9. Se necessário, formate o dispositivo USB com o sistema de arquivos NTFS ou FAT32.

   Digite **format fs=fat32 quick** ou **format fs=ntfs quick**

O dispositivo USB agora está preparado e pronto para uso.

Criar um dispositivo USB de BMR inicializável

Se optar por criar um dispositivo USB de BMR (Bare Metal Recovery - Recuperação Bare Metal) inicializável, você poderá gravar a imagem ISO diretamente em um dispositivo USB para inicializar o novo sistema de computador e permitir que o processo de recuperação bare metal seja iniciado.

Siga estas etapas:

1. Se necessário, prepare o dispositivo USB. Para obter mais informações, consulte Preparar o dispositivo USB (na página 181).
2. Na tela Selecione o método do kit de inicialização, selecione a opção Criar um dispositivo USB de BMR inicializável e clique em Avançar.

   A caixa de diálogo Selecionar a plataforma e o destino é aberta.

3. Selecione a plataforma aplicável para a imagem ISO.

   É possível selecionar qualquer uma das duas opções disponíveis, ou ambas. Se você selecionar as duas plataformas, isso resultará em tempo adicional para criar a imagem.

   Observação: uma imagem ISO criada a partir de uma plataforma de 32 bits deve ser usada para restaurar um servidor de 32 bits. Uma imagem ISO criada a partir de uma plataforma de 64 bits deve ser usada para restaurar um servidor de 64 bits. Se você deseja inicializar um sistema de firmware UEFI, certifique-se de que a opção de plataforma x64 esteja selecionada.

   As opções disponíveis são:

   - Imagem ISO da BMR para plataforma x86 (apenas).
   - Imagem ISO da BMR para plataforma x64 (apenas).
   - Imagem ISO da BMR para plataformas x86 e x64.

4. Especifique a unidade USB.

   Especifique ou procure o local da unidade em que o arquivo de imagem ISO de BMR será criado e gravado no dispositivo USB.

   Observação: para uma unidade USB, se desejar inicializar o sistema de firmware UEFI, você deve formatar a unidade USB como um sistema de arquivos FAT32.

5. Verifique se um dispositivo USB preparado está inserido na unidade especificada.

6. Depois de especificar a plataforma e o local, clique em Avançar.

   A caixa de diálogo Selecionar idiomas é aberta.

7. Selecione o idioma para a imagem ISO de BMR gerada. Durante o procedimento de BMR, a interface do usuário e o teclado estarão integrados com o idioma selecionado.

   Você pode selecionar um ou mais idiomas diferentes para a imagem ISO de BMR. No entanto, cada idioma selecionado resultará em tempo adicional na criação da imagem. Quanto mais idiomas forem selecionados, maior será o tempo levado para a conclusão. Como resultado, você deve selecionar apenas os idiomas realmente necessários.

8. Clique em Avançar.

   A caixa de diálogo Especifique drivers é aberta.

9. Se necessário, selecione a opção Integrar drivers adicionais.

   O painel de driver é ativado e é possível especificar todos os drivers adicionais que você deseja adicionar (ou excluir) da imagem ISO de BMR.

10. Clique em Criar para iniciar o processo e criar uma imagem ISO da BMR inicializável.

    Durante o processo, o status é exibido.

11. Quando o processo for concluído, uma tela de confirmação será exibida para indicar que a imagem ISO de BMR foi gerada e gravada no dispositivo USB com êxito. Essa tela também exibe o local e a plataforma da imagem, juntamente com um link clicável para navegar para esse local.

Verificar se o kit de inicialização foi criado

Após a criação da imagem ISO de BMR com êxito, o utilitário de criação do kit de inicialização exibe um link para a conexão com o local em que a imagem foi salva. Verifique se a imagem ISO de BMR foi salva nesse local. Por padrão, a imagem será salva na pasta Bibliotecas/Documentos, com um formato de nome de imagem padrão composto de:

<PRODUTO>_BMR_<Plataforma>_<OS Kernel>_<versão>(Compilação xxx).ISO

Exemplo:

D2D_BMR_x86x64_w8_r16.5 (Compilação 1234).ISO

Definir um limite para a quantidade de backups simultâneos

É possível definir um limite para a quantidade de tarefas de backup do CA ARCserve D2D executadas simultaneamente. Este recurso permite otimizar o desempenho do servidor proxy da máquina virtual do CA ARCserve D2D no ambiente de backup. Por padrão, o Host-Based VM Backup pode executar até dez tarefas de backup D2D simultaneamente. Em ambientes com várias máquinas virtuais associadas a um sistema do proxy da máquina virtual do CA ARCserve D2D, uma grande quantidade de backups simultâneos podem ter um efeito adverso no desempenho da rede e do backup.

Observação: quando a quantidade de tarefas simultâneas exceder o limite definido, as tarefas que excederem o limite entrarão em uma fila de tarefas.

Siga estas etapas:

1. Efetue logon no sistema proxy da máquina virtual do CA ARCserve D2D.

2. Abra o editor de registro do Windows e procure a seguinte chave de registro:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE D2D
   ```

3. Clique com o botão direito do mouse no CA ARCserve D2D, selecione Novo e clique em String Value no menu pop-up.

   Nomeie a chave como segue:

   ```
   VsphereMaxJobNum
   ```

4. Clique com o botão direito do mouse em VsphereMaxJobNum e clique em Modificar no menu pop-up.

   A caixa de diálogo Editar Cadeia de Caracteres é aberta.

5. No campo Value Data, especifique a quantidade de tarefas de backup do CA ARCserve D2D que deseja que seja executada simultaneamente.

   - **Limite mínimo--**1
   - **Limite máximo--**nenhum.

6. Clique em OK. O limite é definido.
7. Reinicie o serviço web do CA ARCserve D2D.

Aumente a quantidade de mensagens retidas no arquivo de log VMVixMgr

O arquivo de log VMVixMgr mantém as mensagens relacionadas às operações do VMware VIX. Para obter mais informações sobre o API do VMware VIX, consulte o site da VMware.

O arquivo de log VMVixMgr (VMVixMgr.log) está armazenado no seguinte diretório no sistema proxy de backup:

```
C:\Arquivos de Programas\CA\ARCserve D2D\Logs
```

Por padrão, o arquivo de log não pode exceder 500KB. Quando o arquivo de log excede 500KB, as mensagens contidas no arquivo de log serão substituídas. Isso impede que o arquivo de log exceda 500KB.

Ao definir uma programação para fazer backup de dados em intervalos de 15 minutos, é muito provável que o arquivo de log seja substituído quando exceder 500KB. Aumentar o tamanho do arquivo de log permite que você mantenha mais mensagens no arquivo de log.

Como prática recomendada, aumente o tamanho do arquivo de log somente ao definir uma programação para fazer backup de dados a cada 15 minutos.

Siga estas etapas:

1. Efetuar logon no sistema de proxy de backup.
2. Abra o editor de registro do Windows e procure a seguinte chave de registro:

   `HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D`

3. Clique com o botão direito do mouse em CA ARCserve D2D, selecione Novo e clique em DWORD no menu pop-up.

   Nomeie o DWORD como segue:

   `VixMgrLogSize`

   Observação: se o DWORD não estiver presente, o valor padrão para o arquivo de log entra em vigor a 500KB.

4. Após criar o DWORD, clique com o botão direito do mouse em VixMgrLogSize e clique em Modificar no menu pop-up para abrir a caixa de diálogo Editar DWORD.
5. No campo Dados de Valor na caixa de diálogo Editar DWORD, especifique um valor (em KB) do arquivo de log. Por exemplo, 750, 1000 e assim por diante.
6. Clique em OK para aplicar o valor e fechar a caixa de diálogo Editar DWORD.

Proteja o proxy de backup do CA ARCserve D2D

As sessões de backup criadas com o CA ARCserve Central Host-Based VM Backup são armazenadas no proxy de backup. Há várias maneiras de proteger o proxy de backup, dependendo da configuração.

- Se estiver executando o CA ARCserve Central Protection Manager, é possível adicionar o proxy de backup como um nó a ser protegido. Para obter mais informações, consulte o Guia do Usuário do CA ARCserve Central Protection Manager.
- Iniciar a instância do CA ARCserve D2D em execução localmente no proxy de backup e definir as configurações de backup. Selecione toda a máquina como a origem do backup. Para obter mais informações, consulte o Guia do Usuário do CA ARCserve D2D.
- Se estiver executando o CA ARCserve Backup, é possível configurar uma tarefa de backup para proteger o proxy.

Como o processo de instalação afeta os sistemas operacionais

O processo de instalação do CA ARCserve Central Applications atualiza vários componentes do sistema operacional Windows, usando um mecanismo de instalação denominado MSI (Microsoft Installer Package). Os componentes incluídos no MSI permitem que o CA ARCserve Central Applications execute ações personalizadas para instalar ou atualizar o CA ARCserve Central Applications.

A tabela a seguir descreve as ações personalizadas e os componentes afetados:

Observação: todos os pacotes MSI do CA ARCserve Central Applications chamam os componentes listados nesta tabela ao instalar o CA ARCserve Central Applications.

Componente	Descrição
CallAllowInstall	Permite ao processo de instalação verificar condições relativas à instalação atual do aplicativo.
CallPreInstall	Permite ao processo de instalação ler e gravar propriedades do MSI. Por exemplo, ler o caminho de instalação do aplicativo no MSI.
CallPostInstall	Permite ao processo de instalação executar várias tarefas relativas à instalação. Por exemplo, registrar o aplicativo no Registro do Windows.
CallAllowUninstall	Permite ao processo de desinstalação verificar condições relativas à instalação atual do aplicativo.
CallPreUninstall	Permite ao processo de desinstalação executar várias tarefas relativas à desinstalação. Por exemplo, cancelar o registro do aplicativo no Registro do Windows.
CallPostUninstall	Permite que o processo de desinstalação execute várias tarefas depois de desinstalar os arquivos instalados. Por exemplo, a remoção dos arquivos restantes.
ShowMsiLog	Exibe o arquivo de log do Windows Installer no Bloco de notas, caso o usuário final marque a caixa de seleção Mostrar log do Windows Installer nas caixas de diálogo SetupCompleteSuccess, SetupCompleteError ou SetupInterrupted e, em seguida, clique em Concluir. (Funciona somente com o Windows Installer 4.0.)
ISPrint	Imprime o conteúdo de um controle ScrollableText em uma caixa de diálogo. Essa é uma ação .dll personalizada do Windows Installer. O nome do arquivo .dll é SetAllUsers.dll e seu ponto de entrada é PrintScrollableText.

Componente	Descrição
CheckForProductUpdates	Usa o FLEXnet Connect para verificar a existência de atualizações do produto. Essa ação personalizada abre um arquivo executável chamado Agent.exe, que transmite o seguinte: /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Usa o FLEXnet Connect para verificar a existência de atualizações do produto ao reinicializar. Essa ação personalizada abre um arquivo executável chamado Agent.exe, que transmite o seguinte: /au[ProductCode] /EndOfInstall /Reboot

- **Diretórios atualizados -** o processo de instalação instala e atualiza os arquivos do aplicativo nos seguintes diretórios, por padrão:

  `C:\Program Files\CA\`*<application name> (por exemplo, ARCserve Central Applications ou ARCserve D2D)*

  É possível instalar o aplicativo no diretório de instalação padrão ou em um diretório diferente. O processo de instalação copia vários arquivos de sistema para o seguinte diretório:

  `C:\WINDOWS\SYSTEM32`

- **Chaves de registro do Windows atualizadas--**o processo de instalação atualiza as chaves de registro do Windows a seguir:

  Chaves padrão do Registro:

  `HKLM\SOFTWARE\CA\`*<application name> (por exemplo, ARCserve Central Applications ou ARCserve D2D)*

  O processo de instalação cria chaves de registro e modifica várias outras chaves de registro, de acordo a configuração atual do sistema.

- **Aplicativos instalados**--o processo de instalação inclui estes aplicativos em seu computador:

  – Licenciamento CA

  – Microsoft Visual C++ 2010 SP1 redistribuível

  – Java Runtime Environment (JRE) 1.7.0_06

  – Tomcat 7.0.29

Arquivos binários contendo informações incorretas sobre a versão do arquivo

O CA ARCserve Central Applications instala arquivos binários desenvolvidos por terceiros, outros produtos da CA Technologies e o CA ARCserve Central Applications, os quais contém informações incorretas sobre a versão do arquivo. A tabela abaixo descreve tais arquivos binários.

Nome do arquivo binário	Origem
UpdateData.exe	Licença da CA
zlib1.dll	Biblioteca de compactação zlib

Arquivos binários que não contêm um manifesto incorporado

O CA ARCserve Central Applications instala arquivos binários desenvolvidos por terceiros, outros produtos da CA Technologies e o CA ARCserve Central Applications, os quais não contêm um manifesto incorporado nem em texto. A tabela abaixo descreve tais arquivos binários.

Nome do arquivo binário	Origem
BaseLicInst.exe	Licença da CA
UpdateData.exe	Licença da CA
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
tomcat7.exe	Tomcat

Arquivos binários cujo nível de privilégio exige acesso de administrador ao manifesto

O CA ARCserve Central Applications instala arquivos binários desenvolvidos por terceiros, outros produtos da CA Technologies e o CA ARCserve Central Applications com um nível de privilégio de administrador ou o mais alto disponível. É preciso efetuar logon usando uma conta administrativa ou uma conta com o nível de permissão mais alto disponível para executar diversos serviços, componentes e aplicativos do CA ARCserve Central Applications. Os binários correspondentes contêm funcionalidades específicas do CA ARCserve Central Applications, não disponíveis para uma conta de usuário básica. Assim, o Windows solicitará que você confirme uma operação especificando sua senha ou usando uma conta com privilégios administrativos para concluí-la.

- **Privilégios administrativos** - o perfil administrativo ou uma conta com privilégios administrativos têm permissões de leitura, gravação e execução para todos os recursos do Windows e do sistema. Caso não tenha privilégios administrativos, você será solicitado a digitar o nome de usuário e a senha de um usuário administrador para continuar.
- **Privilégios mais altos disponíveis** - uma conta com os privilégios mais altos disponíveis é uma conta de usuário básica e uma conta de usuário avançado que opera com privilégios administrativos.

A tabela abaixo descreve tais arquivos binários.

Nome do arquivo binário	Origem
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications

Nome do arquivo binário	Origem
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Excluir arquivos da verificação do antivírus

O software antivírus pode interferir na execução adequada do aplicativo por meio do bloqueio temporário do acesso aos arquivos ou da quarentena ou exclusão dos arquivos que são classificados incorretamente como suspeitos ou perigosos. É possível configurar a maioria dos softwares antivírus para excluir determinados processos, arquivos ou pastas, de modo a não verificar dados que não precisam ser protegidos. É importante configurar o software antivírus corretamente para que ele não interfira nas operações de backup e de restauração, ou em quaisquer outros tipos de processos.

Os processos, as pastas e os arquivos a seguir devem ser excluídos da verificação do antivírus:

- Lista de processos
  - C:\Arquivos de programas\CA\ARCserve Central Applications\BIN\CCIConfigSettings.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\BIN\CfgUpdateUtil.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\BIN\DBConfig.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\BIN\GetApplicationDetails.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\BIN\GetApplicationDetails64.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\BIN\GetVolumeDetails.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\BIN\VixGetApplicationDetails.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\BIN\VixGetVolumeDetails.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\BIN\GetApplicationDetails64.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\Deployment\Asremsvc.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\Deployment\CheckProdInfo.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\Deployment\DeleteMe.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\Deployment\SetupComm.exe
  - C:\Arquivos de programas\CA\ARCserve Central Applications\Deployment\RestartHost.exe

- C:\Arquivos de programas\CA\ARCserve Central Applications\Update Manager\D2DAutoUpdateUninstallUtility.exe
- C:\Arquivos de programas\CA\ARCserve Central Applications\Update Manager\D2DPMConfigSettings.exe
- C:\Arquivos de programas\CA\ARCserve Central Applications\Update Manager\D2DUpdateManager.exe
- C:\Arquivos de programas\CA\ARCserve Central Applications\Update Manager\UpgradeDataSyncupUtility.exe
- C:\Arquivos de programas\CA\ARCserve Central Applications\TOMCAT\BIN\tomcat7.exe
- C:\Arquivos de programa\CA\ARCserve D2D\TOMCAT\JRE\jre7\bin
  - java.exe
  - java-rmi.exe
  - javaw.exe
  - keytool.exe
  - rmid.exe
  - rmiregistry.exe
- C:\Arquivos de programas(x86)\CA\SharedComponents\CA_LIC
  - CALicnse.exe
  - CAminfo.exe
  - CAregit.exe
  - ErrBox.exe
  - lic98log.exe
  - lic98Service.exe
  - lic98version.exe
  - LicDebug.exe
  - LicRCmd.exe
  - LogWatNT.exe
  - mergecalic.exe
  - mergeolf.exe

Glossário

Arquivo de catálogo

Um arquivo de catálogo é um diretório de informações sobre os dados de backup contidos no banco de dados do CA ARCserve D2D. Para obter mais informações sobre o arquivo de catálogo do CA ARCserve D2D, consulte o *Guia do Usuário do CA ARCserve D2D*.

Detecção automática

A detecção automática é um processo ao qual nós são detectados e adicionados a um ou mais CA ARCserve Central Applications para gerenciamento central.

Diretivas

Uma diretiva é um conjunto de especificações para proteger um nó em um ou mais CA ARCserve Central Applications.

Grupo de nós

Um nó de grupo é um método pelo qual todos os nós gerenciados por um ou mais CA ARCserve Central Applications podem ser organizados por finalidade, por SO ou por aplicativos instalados.

Modo de transporte HOTADD

O modo de transporte HOTADD é um método de transporte de dados que permite fazer backup de máquinas virtuais configuradas com discos SCSI. Para obter mais informações, consulte o Guia de Programação da API do disco virtual no site do VMware.

Modo de transporte NBD

O modo de transporte NBD, também conhecido como modo de transporte LAN, usa o protocolo NFC (Network File Copy - Cópia de arquivos de rede) para estabelecer comunicação. Várias operações do VDDK e VCB usam uma conexão para cada disco virtual acessado em cada host ESX/ESXi Server ao usar o NDB.

Modo de transporte NBDSSL

O modo de transporte NBDSSL (Network Block Device Secure Sockets Layer) usa o protocolo NFC (Network File Copy) para se comunicar. O NBDSSL transfere dados criptografados usando redes de comunicação TCP/IP.

Modo de transporte SAN

O modo de transporte SAN (Storage Area Network) permite a transferência de dados de backup de sistemas proxy conectados à SAN para armazenar dispositivos por meio de comunicação Fibre Channel.

Nó

O nó é uma máquina física ou virtual gerenciada por um ou mais CA ARCserve Central Applications.

Ponto de recuperação

Um ponto de recuperação é uma imagem de backup de blocos de pai mais filho mais antigo. Os backups s filhos ão mesclados com o backup pai para criar novas imagens de ponto de recuperação para que o valor especificado seja sempre mantido.

Proxy de backup

Um proxy de backup é o computador host no qual o CA ARCserve D2D está em execução. O proxy executa as operações de backup configuradas no CA ARCserve Central Host-Based VM Backup.

Sincronização

A sincronização é o processo pelo qual os dados de bancos de dados diferentes são atualizados para que o banco de dados do local central seja consistente com marcas registradas, nós ou sites.

SRM

O SRM (Storage Resource Management) é um recurso que coleta informações sobre dados do aplicativo, dados do hardware e do software ou PKI para o gerenciamento eficiente do ambiente.

Verificação antecipada

O PFC (Preflight Check - Verificação Prévia) é um utilitário que permite executar verificações vitais nos nós para detectar condições que podem ocasionar a falha das tarefas de backup. Você pode exibir os resultados de PFC de um nó ao clicar no ícone na coluna Status de PFC na tela Nó.